Installing and Configuring the Avaya S8500 Media Server

Please disregard any references to the S8710 Media Server in this document. The S8700 Media Server is the currently available product. If you need additional information, please contact your Avaya representative or Avaya authorized business partner.

03-300143
Issue 1
June 2004

Copyright 2004, Avaya Inc.
All Rights Reserved

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support.

Preventing Toll Fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there may be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Disclaimer

Avaya is not responsible for any modifications, additions or deletions to the original published version of this documentation unless such modifications, additions or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

How to Get Help

For additional support telephone numbers, go to the Avaya support Web site: http://www.avaya.com/support. If you are:

- Within the United States, click the *Escalation Management* link. Then click the appropriate link for the type of support you need.
- Outside the United States, click the *Escalation Management* link. Then click the *International Services* link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.
Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").
An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.
Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:
Safety of Information Technology Equipment, IEC 60950, 3rd Edition, or IEC 60950-1, 1st Edition, including all relevant national deviations as listed in Compliance with IEC for Electrical Equipment (IECEE) CB-96A.
Safety of Information Technology Equipment, CAN/CSA-C22.2 No. 60950-00 / UL 60950, 3rd Edition, or CAN/CSA-C22.2 No. 60950-1-03 / UL 60950-1.
Safety Requirements for Customer Equipment, ACA Technical Standard (TS) 001 - 1997.

One or more of the following Mexican national standards, as applicable: NOM 001 SCFI 1993, NOM SCFI 016 1993, NOM 019 SCFI 1998.

The equipment described in this document may contain Class 1 LASER Device(s). These devices comply with the following standards:

- EN 60825-1, Edition 1.1, 1998-01
- 21 CFR 1040.10 and CFR 1040.11.

The LASER devices used in Avaya equipment typically operate within the following parameters:

Typical Center Wavelength	Maximum Output Power
830 nm - 860 nm	-1.5 dBm
1270 nm - 1360 nm	-3.0 dBm
1540 nm - 1570 nm	5.0 dBm

Luokan 1 Laserlaite

Klass 1 Laser Apparat

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposures. Contact your Avaya representative for more laser product information.

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards and all relevant national deviations:

Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.

Information Technology Equipment – Immunity Characteristics – Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11

Power Line Emissions, IEC 61000-3-2: Electromagnetic compatibility (EMC) – Part 3-2: Limits – Limits for harmonic current emissions.

Power Line Emissions, IEC 61000-3-3: Electromagnetic compatibility (EMC) – Part 3-3: Limits – Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems.

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.

This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

REN Number

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For G350 and G700 Media Gateways:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. The digits represented by ## are the ringer equivalence number (REN) without a decimal point (for example, 03 is a REN of 0.3). If requested, this number must be provided to the telephone company.

For all media gateways:

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following tables.

For MCC1, SCC1, CMC1, G600, and G650 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2-T	0.0B	RJ2GX, RJ21X
CO trunk	02GS2	0.3A	RJ21X
	02LS2	0.3A	RJ21X
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9-BN	6.0F	RJ48C, RJ48M
	04DU9-IKN	6.0F	RJ48C, RJ48M
	04DU9-ISN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9-DN	6.0Y	RJ48C

For G350 and G700 Media Gateways:

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground Start CO trunk	02GS2	1.0A	RJ11C
DID trunk	02RV2-T	AS.0	RJ11C
Loop Start CO trunk	02LS2	0.5A	RJ11C
1.544 digital interface	04DU9-BN	6.0Y	RJ48C
	04DU9-DN	6.0Y	RJ48C
	04DU9-IKN	6.0Y	RJ48C
	04DU9-ISN	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

For all media gateways:

If the terminal equipment (for example, the media server or media gateway) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. It is recommended that repairs be performed by Avaya certified technicians.

The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

This equipment, if it uses a telephone receiver, is hearing aid compatible.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Declarations of Conformity

United States FCC Part 68 Supplier's Declaration of Conformity (SDoC)

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

All Avaya media servers and media gateways are compliant with FCC Part 68, but many have been registered with the FCC before the SDoC process was available. A list of all Avaya registered products may be found at: http://www.part68.org by conducting a search using "Avaya" as manufacturer.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://www.avaya.com/support.

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

To order copies of this and other documents:

Call: Avaya Publications Center
Voice 1.800.457.1235 or 1.207.866.6701
FAX 1.800.457.1764 or 1.207.626.7269

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attention: Avaya Account Management

E-mail: totalware@gwsmail.com

For the most current versions of documentation, go to the Avaya support Web site: http://www.avaya.com/support.

Contents

About this Documentation 9

- Audience 9
- Using this documentation 9
- Conventions 10
  - General 10
  - Physical dimensions 10
  - Terminology 10
  - Typography 10
    - Commands 11
    - Keys 11
    - User input 11
    - System output and field names 12
- Downloading this book and updates from the Web 12
  - Downloading this documentation 12
- Safety labels and security alert labels 13
- Safety precautions 13
- Related resources 16
- Technical assistance 16
  - Within the US 16
  - International 16
- Trademarks 16
- Sending us comments 16

1 Introduction 19

- Pre-installation information 19
  - Before you go on site 19
    - Downloading license and Avaya authentication files 20
    - Copying files to the laptop 21
  - Before you start the installation 21
- Equipment specifications 22
- Required hardware 24
- Remote Supervisor Adapter 26
  - Remote Supervisor Adapter components 26
- Documentation 27

- Connecting to the customer's network 28
- Connecting the modems 29
- High level overview of installation process 31
  - Installing and cabling the media server complex 31
  - Installing Avaya Communication Manager 31
  - Configuring the maintenance adapter 31
  - Configuring the media server 31
  - Translating the IPSIs 31
  - Installing and cabling the media gateways 32
  - Completing the installation administration 32
  - Testing the complete installation 32

2 Configuring the hardware in the rack 33

- Configuring the SNMP modules in the UPS 34
  - Single control network 35
  - Setting selected traps (alarming) 36
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) 37
- Configuring the media server 39
  - Clearing the ARP cache on the laptop 39
  - Disabling the RSA loader watchdog 40
  - Powering up the media server 41
  - Accessing the media server 41
  - Setting up Telnet 41
  - Installing Avaya Communication Manager 42
  - Using the Installation Wizard 43
  - Verifying media server connection to the customer's LAN (if provided) 45
  - Configuring the modem 46
  - Checking LED activity on the optional dual NIC 48
  - Disconnecting from the media server 48
- Configuring the dual NIC 49
  - Configuring the NIC 49
  - Testing connectivity to customer's network 50
- Configuring the maintenance adapter 52
  - Connecting and logging into the adapter 52
  - Adding login IDs and passwords 53
  - Configuring Advanced System Management 54
  - Setting alarms 55
  - Verifying network interfaces 57

Restart ASM 57
Backing up the configuration 57
Setting auto answer on the RSA 59
Enabling the RSA loader watchdog 60
Logging off the RSA 60

3 Connecting to the IPSIs 61

- Programming the IPSI circuit packs 61
- Verifying that IPSIs are translated 66
- Verifying connectivity to media server 66
- Upgrading IPSI firmware version (if necessary) 67
- Enabling control of IPSIs 67
- Verifying license status 67
- Reusing a TN2312AP/BP circuit pack 68

4 Translating the IPSIs 69

- Starting terminal emulation 69
- Inputing translations 70
- Resetting the media server 70
- Adding media gateways 70
- Administering the IPSIs 71
  - Adding IPSI information 72
  - Setting alarm activation level 72
  - Installing the translation file 73

5 Completing the installation administration 75

- Verifying translations 75
- Setting daylight savings time rules 76
- Setting locations (if necessary) 77
- Verifying date and time 77
- Resolving alarms 78
- Backing up files to the compact flash media 78
- Telneting to media server 80
- Enabling alarms 80
  - To INADS via modem 80
  - To INADS via SNMP 80

- Registering the system 81

6 Installing the media gateways 83

7 Testing the media server installation 85

- Testing the TN2312BP IPSI circuit pack 85
- Testing the license file 86
- LED indicators 87
  - Avaya S8500 Media Server LEDs 88
  - Avaya Ethernet switch LEDs 89
  - Uninterruptible power supply LEDs 90
  - IPSI LEDs 90

A Accessing the media server 95

- Connecting to the media server directly 95
- Connecting to the media server remotely over the network 97
- Connecting to the media server remotely over a modem 97
  - Setting up a dial-up connection 97
  - Dialing up to the media server 98
- Accessing the Maintenance Web Interface 98
- Using the command line interface 98
- Logins 99
- Network configuration 100
- Browser settings 101
  - Connecting directly to the media server 101
  - Connecting remotely through the network 101

B Troubleshooting an installation 103

- Installing the media server hardware 103
- Configuring the media server hardware 104
- Installing the license and Avaya authentication files 105

C Avaya RSA defaults 107

Index 113

About this Documentation

This documentation, *Installing and Configuring the Avaya S8500 Media Server* (03-300143) provides procedures for installing Avaya Communication Manager and configuring an S8500 Media Server and other control network components.

Audience

This documentation is for the following people tasked with installing and configuring the media server components:

- Trained field installation and maintenance personnel
- Technical support personnel
- Authorized Business Partners

Using this documentation

Use this documentation as a guide to install and configure the S8500 Media Server. For information about a particular task, use the index or table of contents to locate the page number where the information is described.

For an overview of the installation process, see High level overview of installation process on page 31.

Read Pre-installation information on page 19 first. This section lists all tasks that must be completed before beginning the procedures described in this document. One step you normally complete before going to the customer site is getting the license and Avaya authentication files from the Remote Feature Activation (RFA) Web site.

For technical specifications on the hardware, see Table 2, Avaya S8500 Media Server features and specifications, on page 22.

For the physical installation and cabling of the hardware, see the *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701). Use the remaining sections of the document in the sequence they are presented. If certain components are not to be installed, skip the procedures for those components. You install and configure the media server components using information in the following sections:

- Configuring the SNMP modules in the UPS on page 34
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 37
- Configuring the media server on page 39
- Configuring the dual NIC on page 49
- Configuring the maintenance adapter on page 52
- Translating the IPSIs on page 69
-

You next install the media gateways, using sections in *Installing the Avaya G650 Media Gateway* (03-300144).

Connect the system to the customer's network using information in Connecting to the IPSIs on page 61.

Complete the installation using information in the following sections:

- Completing the installation administration on page 75
- Testing the media server installation on page 85
- Accessing the media server on page 95

If problems occur during the installation, use Troubleshooting an installation on page 103 to try to resolve them.

Conventions

This section describes the conventions that we use in this book.

General

We show commands and screens from the newest MultiVantage system and refer to the most current books. You must substitute the appropriate commands for your system and refer to the books that you have available.

Physical dimensions

All physical dimensions in this book are in English units followed by metric units in parentheses. Wire gauge measurements are in AWG followed by the diameter in millimeters in parentheses.

Terminology

We use the following terminology in this documentation:

- *Configuration* is a general term that encompasses all references to an Avaya media server with media gateways running Avaya Communication Manager.
- *Cabinet* refers to a stack of media gateways (such as the G650) that are TDM-cabled together.
- *UUCSS* refers to a circuit pack address in cabinet-carrier-slot order.

Typography

This section describes the typographical conventions for commands, keys, user input, system output, and field names.

Commands

- Commands are in **bold san serif** type.

  Example

  Type **change-switch-time-zone** and press **Enter**.

- Command variables are in ***bold sans serif italic*** type when they are part of what you must type, and in *plain italic* type when they are not part of what you must type.

  Example

  Type **ch ma machine_name**, where *machine_name* is the name of the call delivery machine.

- Command options are in **bold** type inside square brackets.

  Example

  At the DOS prompt, type ***copybcf [-F34]***.

Keys

The names of keys are in bold type.

Example

Use the **Down Arrow** key to scroll through the fields.

When you must press and hold a key and then press a second or third key, we separate the names of the keys with a plus sign (+).

Example

Press **ALT+D**.

When you must press two or more keys in sequence, we separate the names of the keys with a space.

Example

Press **Escape J**.

When you must press a function key, we provide the function of the key in parentheses after the name of the key.

Example

Press **F3** (Save).

User input

User input is in **bold** type, whether you must type the input, select the input from a menu, or click a button or similar element on a screen or a Web page.

Examples

- Type **exit**, and then press **Enter**.
- On the **File** menu, click **Save**.
- On the Network Gateway page, click **Configure** > **Hardware**.

System output and field names

System output and field names on the screen are in `monospaced` type.

Example

- The system displays the following message:

  ```
  The installation is in progress.
  ```

Field names on the screen are in **bold sans serif** type.

Example

- Type **y** in the **Message Transfer?** field.:

Downloading this book and updates from the Web

You can download the latest version of this documentation from the Avaya Support Web site (http://support.avaya.com). You must have access to the Internet and a copy of Adobe Reader installed on your personal computer.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this documentation. Therefore, the Avaya Support Web site might also contain new product information and updates to the information in this book. You also can download these updates from the Avaya Support Web site.

Downloading this documentation

To download the latest version of this documentation:

1. Access the Avaya Support Web site at http://support.avaya.com.
2. Type the documentation number in the Search Support box in the upper left and click **Go**.

   The system displays the Product Documentation Search Results page.
3. Or click **Product Documentation**.
4. From the menu on the left, select Communications Systems.
5. Scroll down to find the product and latest release number.
6. Click the release number to view the list of titles.
7. Click on the title that you want.
8. Click one of the following options:
   - **PDF Format** to download the book in regular PDF format.
   - **ZIP Format** to download the book in zipped PDF format.

Safety labels and security alert labels

Observe all caution, warning, and danger statements to help prevent loss of service, equipment damage, personal injury, and security problems. This book uses the following safety labels and security alert labels:

CAUTION:
A caution statement calls attention to a situation that can result in harm to software, loss of data, or an interruption in service.

WARNING:
A warning statement calls attention to a situation that can result in harm to hardware or equipment.

Use an ESD warning to call attention to situations that can result in ESD damage to electronic components.

DANGER:
A danger statement calls attention to a situation that can result in harm to personnel.

SECURITY ALERT:
A security alert calls attention to a situation that can increase the potential for unauthorized use of a telecommunications system.

Safety precautions

DANGER:
Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.

Connect all power cords to a properly wired and grounded electrical outlet.

Connect to properly wired outlets any equipment that will be attached to this product.

When possible, use one hand only to connect or disconnect signal cables.

Never turn on any equipment when there is evidence of fire, water, or structural damage.

Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the

installation and configuration procedures.

Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

To connect:		To disconnect:	
1	Turn everything off.	**1**	Turn everything off.
2	Attach all cables to devices.	**2**	Remove power cords from outlet.
3	Attach signal cables to connectors.	**3**	Remove signal cables from connectors.
4	Attach power cords to outlet.	**4**	Remove all cables from devices.
5	Turn device ON.		

DANGER:

Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following:

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

CAUTION:

When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.

Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

CAUTION:

Use safe practices when lifting.

CAUTION:

The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one connection to the power. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

CAUTION:

If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to an easily accessible power source.

CAUTION:
Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. Only a qualified service technician is authorized to remove the covers where the following label is attached.

CAUTION:
Do not place any object weighing more than 180 lb. (82 kb) on top of rack-mounted devices.

CAUTION:
Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your Remote Supervisor Adapter (RSA) for electrical specifications.

CAUTION:
Make sure that the rack is secured properly to avoid tipping when the media server is extended.

CAUTION:
To reduce the risk of electric shock or energy hazards:

This equipment must be installed by trained service personnel in a restricted-access location, as defined by the NEC and IEC 60950, Third Edition, The Standard for Safety of Information Technology Equipment.

Connect the equipment to a reliably grounded safety extra low voltage (SELV) source. An SELV source is a secondary circuit that is designed so that normal and single fault conditions do not cause the voltages to exceed a safe level (60 volts DC).

The branch circuit overcurrent protection must be rated at a minimum of 5 amperes to a maximum of 15 amperes.

Use 14 American Wire Gauge (AWG) or 2.5 mm^2 copper conductor only, not exceeding 3 meters in length.

Torque the wiring-terminal screws to 12 inch-pounds (1.4 newton-meters).

Related resources

For providing physical installation and connection information, see *Quick Start for Hardware Installation: Avaya S8500 Media Server,* 555-245-701.

Additional information on installing some adjunct and peripheral equipment that an S8500 media server supports is contained in *Adding New Hardware—S8500, S8700, and S8710 Media Servers* (555-233-112).

For all documents associated with the S8500 Media Server, including those described above, see *Documentation for Avaya Communication Manager, Media Gateways and Servers* CD (03-300151).

Technical assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with:

- Feature administration and system applications, call the Avaya DEFINITY Helpline at 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

Avaya Inc.
Product Documentation Group
Room B3-H13
1300 W. 120 Ave.
Westminster, CO 80234 USA

- E-mail, send your comments to:

  document@avaya.com

- Fax, send your comments to:

  1-303-538-1741

Ensure that you mention the name and number of this book, *Installing and Configuring the Avaya S8500 Media Server* (03-300143).

1 Introduction

These procedures are for installing Avaya Communication Manager and configuring a new Avaya S8500 Media Server and associated components in either an IP Connect or direct connect configurations.

As part of the procedures for configuring the various pieces of hardware, you use two administration interfaces: the Maintenance Web Interface and a command line interface using either telnet or a terminal emulation program such as Avaya Native Configuration Manager. You also use the Avaya Installation Wizard to configure the media server.

There are no requirements to install the media server before the media gateways; however, the license file only allows 30 minutes to "see" the administered and connected IP Server Interface circuit packs.

The following information is included in this installation procedure:

- Pre-installation information on page 19
- High level overview of installation process on page 31
- Configuring the SNMP modules in the UPS on page 34
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 37
- Configuring the media server on page 39
- Configuring the dual NIC on page 49
- Configuring the maintenance adapter on page 52
- Translating the IPSIs on page 69
- Connecting to the customer's network on page 28
- Connecting to the IPSIs on page 61
- Completing the installation administration on page 75
- Installing the media gateways on page 83
- Testing the media server installation on page 85
- Accessing the media server on page 95
- Troubleshooting an installation on page 103

Pre-installation information

Before you go on site

Before going on site, make sure the customer has a local area network set up and running and a network administrator available the day of the installation. Before beginning the software installation and media server configuration, make sure you have the filled-out *Electronic Preinstallation Worksheet* (EPW) on the services laptop. See the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw) for the blank form.

In addition, the pre-installation team should have done the following tasks. If they were not all done, do not continue with the installation.

- Verify that the services laptop has the right hardware and software. See Connecting to the media server directly on page 95 for the list of computer hardware and software specifications.
- Verify that you have current translations available for download via ProVision.
- Verify that you have a filled-out *Electronic Preinstallation Worksheet* (EPW). The EPW provides
  - IP addresses
  - Product ID (same for both media server and Remote Supervisor Adapter [RSA])
  - Avaya services telephone number for remote access over modem
  - Avaya services IP address for alarms through the network
- Verify that you have the current software update (patch), if required, and license and Avaya authentication files on your services laptop.
- Verify that you have the current firmware available, including for the BIOS and RSA. Firmware for the IPSIs, C-LAN, MedPro, and VAL circuit packs are on the software CD, but check the Avaya Support Web site (http://support.avaya.com), Download Software and Firmware, for the latest software and firmware.
- Verify that you have all the login IDs and passwords to access the S8500 Media Server, maintenance adapter, and server complex components. This includes the unique service password for that customer's equipment.

  To obtain the password for a specific media server, call ASG Conversant (1.800.248.1234 or 1.720.444.5557). You must have the IL, FL, or product ID to get the password.

  To log in through the services port as craft after you install the Avaya authentication file, use this password, which does not require an ASG challenge or response.

Downloading license and Avaya authentication files

Use the Remote Feature Activation (RFA) to obtain the license and Avaya authentication files. RFA is a Web-based application, available to Avaya employees and authorized Business Partners, that enables you to create and deploy license files for all product platforms. The RFA Web site is at http://rfa.avaya.com. For specific information on RFA and how to generate license and Avaya authentication files, go to the the RFA Information page available on the RFA Web site.

> **NOTE:**
> To access the RFA application, you must take the RFA online training and pass the online test.

To generate a license file, you need the following information:

- Your personal Single Sign-On (SSO) for the RFA Web site authentication login.
- SAP order number
- Required customer information
- Serial number of one TN2312BP Internet Protocol Server Interface (IPSI) circuit pack designated the reference IPSI.
- Intranet access to the RFA Web page with Internet Explorer 5.0 or higher.

Before arriving on site, download the license and Avaya authentication files to the services laptop. The license and Avaya authentication files are installed during the installation process.

Once the Avaya authentication files are installed, Avaya services logins to the media server are protected by a challenge/response system called Access Security Gateway (ASG). The ASG challenge/response protocol confirms the validity of each user, reducing the opportunity for unauthorized access.

When finished installing the Avaya authentication file, Avaya Communication Manager has a password for the craft login. This password is unique to the customer's server. You can use the password the next time you log in as craft, provided you access the media server through the services port. You do not need an ASG challenge/response to log in this way, even though every other means of craft access still require an ASG challenge/response. The revised password is recorded by RFA and is obtained from ASG Conversant at 1-800-248-1234 or 1-720-444-5557.

Copying files to the laptop

In addition to the license and Avaya authentication files, you must copy other required files to the services laptop. This includes the filled-out *Electronic Preinstallation Worksheet* (EPW); any software updates; current firmware, including firmware for the BIOS, maintenance adapter, and programmable circuit packs.

To get a filled-out EPW, go to the project manager or customer. To get a blank EPW, go to the Avaya Installation Wizard Web site (http://support.avaya.com/avayaiw). Have the customer fill it out.

To get the software update (patch), go to the Avaya Support Web site (http://avaya.com/support) and select **Software & Firmware Downloads** to identify and copy the required software update.

To get the latest firmware for the BIOS, maintenance adapter, and programmable circuit packs, go to the Avaya Support Web site at http://avaya.com/support and select **Software & Firmware Downloads** to identify and copy the latest firmware.

Before you start the installation

The pre-installation team should have done the following tasks. If they were not all done, do not continue with the installation.

- Verify that the open, customer-supplied, EIA-310D (or equivalent) standard 19-in. (48-cm) 4-post equipment rack(s) is(are) properly installed and solidly secured. Make sure that the screws that come with the racks are there. If using a rack cabinet, make sure it has adequate ventilation.
- Verify that the rail kit to support the S8500 Media Server is available for installation.
- Verify that the rail kits, required to support the very heavy UPSs, are installed on the rack or available for installation. For information on installing the rails, see the documentation that comes with the rail kits.
- Verify that the equipment rack(s) is(are) grounded per local code. See *Job Aid: Approved Grounds* (555-245-772).
- Verify that the customer provides AC power to the rack from a nonswitched outlet.
- Verify that cabling for the TN2312BP IP Server Interface (IPSI) circuit packs is labeled and run from the control hardware rack to the port networks or that appropriate connectivity is provided.
- Verify that you have all the equipment on site. See Table 3, List of required hardware, on page 24 for the list of required hardware.

Equipment specifications

The media server control network components consist of the media server, one UPS, and an Avaya-provided Ethernet switch (optional). See Table 1, Control network components specifications, on page 22.

Table 1: Control network components specifications

Component	Dimensions English (in)	Metric (cm)	Us (height in rack)	Weight (lb/kg)
S8500 Media Server	1.75h x 17d x 17w	4.4h x 43d x 43w	1	23/10.5
Ethernet Switch:				
P133G2/P134G2	3.5h x 14d x 19w	9h x 35d x 48w	2	11,13/5,6
P333T/334T	3.5h x 18d x 19w	9h x 45d x 48w	2	16.5/7.5
UPS:				
700 VA	3.5h x 19d x 17w	9h x 48d x 43w	2	34/15
1500 VA	3.5h x 24d x 17w	9h x 30d x 43w	2	50/23

The internal room temperature must not exceed 104° F (40° C).

Table 2, Avaya S8500 Media Server features and specifications, on page 22 outlines the features and specifications of the Avaya S8500 Media Server.

NOTE:
Some values are shown at maximum configuration. Avaya values will be slightly lower then the maximum.

Table 2: Avaya S8500 Media Server features and specifications *1 of 3*

Features and specifications	Description
Microprocessor	One Pentium 4 512-KB Level-2 cache and MMX (MMX2) technology
Memory	256 MB Type: PC2100 266 MHz, ECC SDRAM, registered DIMMs only Slots: Four dual inline
Drives	Diskette: 1.44 MB CD-ROM: IDE
Power Supply	203 watt (110 or 220 VAC auto-sensing)

Table 2: Avaya S8500 Media Server features and specifications ***2 of 3***

Features and specifications	Description
Physical Dimensions	Height: 1.75 inches (4.4 millimeters, 1 U) Depth: 17 inches (43 millimeters) Width: 17 inches (43 millimeters) Maximum weight: 23 lb (10.5 kg)
Integrated Functions	Ethernet ports: Two 1000/100/10Base-T Ethernet controllers One serial port Two USB ports Keyboard port Mouse port Dual-channel bus mastering IDE controller Diskette drive
Acoustical Noise Emissions	Sound power, idling: 6.5 bel maximum Sound power, operating: 6.5 bel maximum
Environment: Air Temperature	Server on: 50.0° to 95.0° F (10° to 35° C) altitude: 0 to 2,998.7 feet (914 meters) Server off: -40° to 140° F (-40° to 60° C) maximum altitude: 6,998.0 feet (2,133 meters)

Table 2: Avaya S8500 Media Server features and specifications ***3 of 3***

Features and specifications	Description
Environment: Humidity	Server on: 8% to 80% Server off: 8% to 80%
Heat Output	BTU output per hour (approximate): Maximum configuration: 512 BTU (150 watts)
Electrical Input	Sine-wave input (47-63 Hz) required Input voltage low range: Minimum: 100 VAC Maximum: 127 VAC Input voltage high range: Minimum: 200 VAC Maximum: 240 VAC Input kilovolt-amperes (kVA) (approximate): Minimum: 0.0870 kVA Maximum: 0.150 kVA Receptacle U.S.: XXXX 87=NEMA 5-15 Circuit Breaker: XXXX 87=15 amp Pole: XXXX 87=1 Amp Draw: XXXX 87=3

Required hardware

Before beginning the process, make sure you have the hardware listed in Table 3, List of required hardware, on page 24 and Table 4, List of optional localization kits, on page 25 on hand.

Table 3: List of required hardware

Comcode	Description	Number	Included	Optional	FRU
700262629	S8500 Media Server with AC power	1	Yes		Yes
408357002 408427409 700181928	Powerware 9125 uninterruptible power supply (UPS) (if Avaya-provided) – US & Canada – International – Japan	1		Yes (can be customer provided)	Yes
408427656	SNMP Network Interface Adapter for UPS (if Avaya-provided)	1		Yes	Yes
700230741	Rail kits for mounting UPSs in rack – 4-post rack (Powerware code: 05146726-5501)	1		Yes	Yes

Table 3: List of required hardware

Comcode	Description	Number	Included	Optional	FRU
108873233 108563123 108644451	10/100BaseT Ethernet switch (if Avaya-provided) – Avaya Ethernet P133 switch – Avaya Ethernet P333 switch – Avaya Ethernet P334 switch	1		Yes	Yes
700169121	External V.90 56K USB modem with cable (if used)	1	Yes		Yes
700277551	Serial modem (requires one localization kit)	1	Yes		Yes
700289580	Compact flash disk memory reader	1	Yes		Yes
N/A	Compact flash disk	1		Yes	Yes
N/A	Dual Network Interface Card (NIC)	1	Yes (if only 1 port network)	Yes	Yes
700287964	Avaya Communication Manager CD for Linux Servers		Yes		Yes
700277726	Avaya S8300, S8500, S8700 Media Server Library CD (555-233-824)		Yes		Yes
700170012 700178056 700178064	Green CAT5 Ethernet cables – 5-meter (16 feet) – 25-meter (82 feet) – 50-meter (164 feet)	4 2-68 2-68	Yes		Yes
700170053	Black CAT5 Ethernet crossconnect cable for laptop computer		Yes		Yes
407063478	Electrostatic discharge (ESD) wrist strap	1	Yes		Yes

Table 4: List of optional localization kits

Comcode	Description	Number	Included	Optional	FRU
700277569	Localization kit LK-ZBA-US			Yes	Yes
700277577	Localization kit LK-ZBA-EURO			Yes	Yes
700277585	Localization kit LK-ZBA-AU			Yes	Yes
700277601	Localization kit LK-ZBA-BE			Yes	Yes
700277619	Localization kit LK-ZBA-CH			Yes	Yes
700277627	Localization kit LK-ZBA-DE			Yes	Yes
700277635	Localization kit LK-ZBA-DK			Yes	Yes
700277643	Localization kit LK-ZBA-FI			Yes	Yes
700277650	Localization kit LK-ZBA-FR			Yes	Yes
700277668	Localization kit LK-ZBA-GB/IE			Yes	Yes

Table 4: List of optional localization kits

Comcode	Description	Number	Included	Optional	FRU
700277676	Localization kit LK-ZBA-IN+			Yes	Yes
700277684	Localization kit LK-ZBA-IT			Yes	Yes
700277692	Localization kit LK-ZBA-NL			Yes	Yes
700277700	Localization kit LK-ZBA-NZ			Yes	Yes
700277718	Localization kit LK-ZBA-SE/IS			Yes	Yes

Remote Supervisor Adapter

The RSA monitors and reports alerts on the Avaya S8500 Media Server components and provides control to power-on and power-off the S8500. Using a browser, the Advanced System Management (ASM) Web interface administers the RSA.

The RSA is installed in PCI-X slot 1 of the Avaya S8500 Media Server. Although all the software needed to use the RSA comes installed from the factory, you still need to configure the RSA before you use it. The RSA comes loaded from the factory with Avaya defaults. Not all fields could be set to a default.

NOTE:
Only the fields that need to be added or changed for an Avaya installation are outlined in this section. Fields that contain the Avaya defaults that do not need to be modified can be found in Avaya RSA defaults on page 107. Detailed information on all the RSA fields can be found in the *Avaya Remote Supervisor Adapter User Guide* (555-245-702).

WARNING:
Executing the **Restore Defaults** option in the navigation pane removes the Avaya defaults. Avaya defaults can be restored manually using the information found in Avaya RSA defaults on page 107 or by restoring the default file. The Avaya default file can be found at http://support.avaya.com or on the Avaya Communication Manager 2.0 CD for Linux Servers and Gateways. For instructions on restoring the default file, see the Configuration File in the *Avaya Remote Supervisor Adapter User Guide* (555-245-702).

The RSA uses a separate serial modem to forward alerts to alert recipients and for remote access. It also uses its own connection to the customer's network to provide SNMP alerts.

Remote Supervisor Adapter components

See Figure 1, Connector panel on the Remote Supervisor Adapter, on page 27 for locations of the connectors and components of the RSA. See Table 5, Remote Supervisor Adapter components, on page 27 for a detailed description of the components and connectors.

Figure 1: Connector panel on the Remote Supervisor Adapter

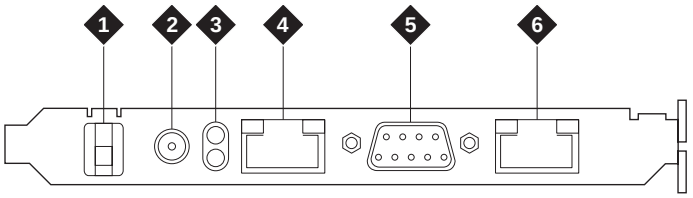


Figure notes

1	Clip	**4**	ASM RS-485 RJ14 connector
2	External power-supply connector	**5**	Serial connector
3	Power and error LEDs	**6**	Ethernet RJ45 connector

Table 5: Remote Supervisor Adapter components

RSA component	Description
Clip	Power cord retaining clip
External power-supply connector	Connect the power-supply adapter to this connector. A power cord connects from the power-supply adapter to the power source. This connection provides power to the RSA that is independent of the Avaya S8500 Media Server power supply.
Power and error LEDs	The GREEN LED: Shows the status of the power connection. The AMBER LED: Shows that an error condition exists on the RSA.
Ethernet RJ-45 connector	A 10/100 Mbps connector for LAN connectivity.
Serial connector	Used for serial modem connectivity.
ASM RS-485 RJ-14 connector	Not used in the Avaya S8500 Media Server configuration.

Documentation

We recommend that you have the following documents on hand for the installation. These are included on the *Documentation for Avaya Communication Manager, Media Gateways and Servers* CD (03-300151).

- *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701)—a quick reference guide providing physical installation and connection information.
- Filled-out *Electronic Preinstallation Worksheet*—An Excel spreadsheet providing the customer's network information needed to use the Avaya Installation Wizard to configure the control network components. Get from the Avaya project manager, Avaya software technician, or customer network administrator. A blank one is available at the AIW Web site (http://support.avaya.com/avayaiw).

- *Installing and Configuring the Avaya S8500 Media Server* (03-300144)—this document, providing information on configuring the control network components, testing, and troubleshooting.
- *Avaya Remote Supervisor Adapter Users' Guide* (555-245-702)—documentation providing information on administering the RSA.
- *Job Aid: Approved Grounds* (555-245-772)—job aid providing a description of all approved grounds.
- *Upgrading Software and Firmware—Avaya S8500 Media Server* (555-245-111)—part of the library providing information on upgrading Avaya Communication Manager and firmware for various components and circuit packs.
- *Administrator's Guide for the Avaya Communication Manager (555-233-506)*—end-user documentation that includes information on administering trunks and telephones.
- *Administration for Network Connectivity for the Avaya Communication Manager* (555-233-124)—documentation providing information on network connectivity.
- *Maintenance Alarms for Avaya Communication Manager 2.1, Media Gateways and Servers* (03-300190)—provides information on how to troubleshoot and replace various components.
- *Maintenance Commands for Avaya Communication Manager 2.1, Media Gateways and Servers* (03-300191)—provides information on how to use command interfaces, command syntax, and output from maintenance-related commands.
- *Maintenance Procedures for Avaya Communication Manager 2.1, Media Gateways and Servers (*03-300192)—provides information on how to use alarms, error codes, and tests to diagnose and repair problems.

Connecting to the customer's network

The media server connects directly to the customer's network. In a typical configuration you connect to the customer's network through a port on the back of the Avaya S8500 Media Server, using a standard CAT5 cable with RJ45 connectors on each end. Typically, you connect through port 1 (Eth0). The other end of the cable connects to an Ethernet switch (router), hub, or token ring.

If the S8500 Media Server has only one port network, you connect it through the dual NIC. See Figure 2, CAT5 cable connected to a port on the back of the Avaya S8500 Media Server, on page 29 for connectivity information.

Figure 2: CAT5 cable connected to a port on the back of the Avaya S8500 Media Server

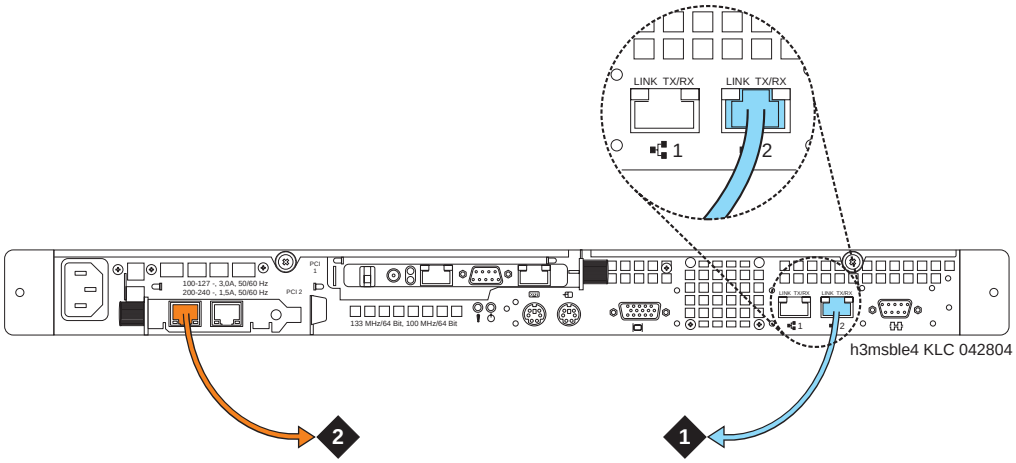


Figure notes

1 To network (if nondedicated control network)

2 To port network if only one or to network (if dedicated control network)

Connecting the modems

There are two modems on an Avaya S8500 Media Server configuration. One modem connects to the USB port on the front of the Avaya S8500 Media Server. The other modem connects to the RS-232 port on the RSA. If you have not connected the modems yet, do so now.

NOTE:
USB and serial modems cannot connect to rotary lines. A Touch Tone line is required.

Required options on the USB modem are set by the operating system on the media server. Required options on the RSA modem are set by Avaya defaults on the RSA. There are no options to set on either modem.

The modems for the media server and the RSA share one dedicated telephone line. The modem on the media server always answers an incoming call if the media server is healthy. In the event the media server is down, the modem on the RSA answers the incoming call. For a modem connectivity diagram see Figure 3, Modem connectivity on the Avaya S8500 Media Server, on page 30 .

Figure 3: Modem connectivity on the Avaya S8500 Media Server

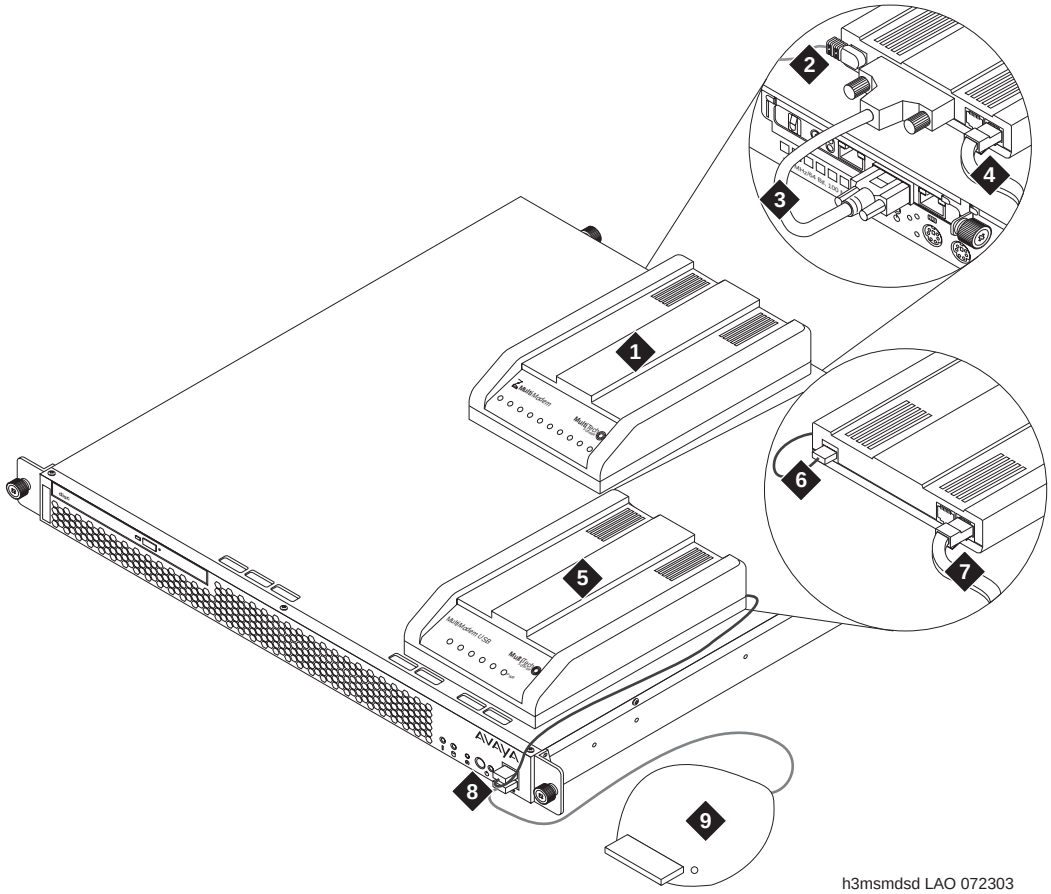


Figure notes

1 Serial modem

2 Power cord

3 Serial modem cable connecting the serial modem to the RS-232 port on the RSA.

4 Telephone line connecting the serial modem to the outside line.

5 USB modem used for Avaya Communication Manager.

6 USB cable connecting the USB modem to the USB port on the media server.

7 Telephone line connecting the USB modem to the outside line.

8 2 USB ports on the front of the media server.

9 Compact flash memory reader connecting to the USB port on the media server.

1 Terminate the 1-MB telephone line at the RJ11 jack outlet.

2 Connect the telephone line to the modems with the modular telephone cord supplied with each modem.

3 Connect the USB cable from the USB modem to one of the USB ports on the front of the Avaya S8500 Media Server.

4 Connect the serial cable from the serial modem to the RS232 port on the RSA card.

5 Connect the power cords from each modem to the power outlet.

High level overview of installation process

The installation process is completed in stages. Some stages can be completed in parallel, and others require that certain tasks be accomplished before the stages can be completed. The order that the particular stages are completed depends on local practice and the personnel available. The high level stages are listed below.

Installing and cabling the media server complex

You can complete this stage before, in parallel with, or after installing the media gateways. See the *Quick Start for Hardware Installation: Avaya S8700 or S8710 Media Server* (555-245-703)

Installing Avaya Communication Manager

The media server is shipped with a blank hard drive. The operating system, directories, and files needed for the media server are installed from a bootable CD containing the operating system and Avaya Communication Manager. This stage is usually done immediately after installing the media server hardware.

Configuring the maintenance adapter

The maintenance adapter, which for this release is the Remote Supervisor Adapter (RSA), monitors various components and environmentals on the media server. The adapter comes installed from the factory with Avaya defaults but must be configured to fit your specific installation. You administer the adapter through its own Web interface. You set the IP address for the adapter when you configure the media server through the Avaya Installation Wizard.

Configuring the media server

Use the Avaya Installation Wizard to configure the media server. You must have the filled-out *Electronic Preinstallation Worksheet* (EPW) that provides the customer's network information needed for configuring the network components. As part of the Wizard, you install the license and Avaya authentication files. This stage is done after installing the software.

Translating the IPSIs

This stage is done after the media server is configured. Once the license file is installed (as part of the Avaya Installation Wizard), you have 30 minutes to complete this step before the license file looks for the reference IPSI.

Installing and cabling the media gateways

You can do this stage before, in parallel with, or after installing and configuring the media server complex. The media gateways must be installed and powered up to effectively complete many of the other stages. The IPSI circuit packs can only be programmed in a powered up media gateway.

Completing the installation administration

This stage finishes the installation. Clearing alarms, enabling alarm reporting, backing up the server files, and registering the configuration. This stage always comes at the end of the complete installation.

Testing the complete installation

This stage verifies the complete configuration operation and is the last task.

2 Configuring the hardware in the rack

Once the control network equipment is installed and connected, you must configure the media server, the SNMP Module in the UPS (if Avaya supplied), and the SNMP Subagent in the Avaya Ethernet switch (if Avaya supplied). The latter two are to allow that equipment to send alarms (traps) to the media server.

Configure the SNMP agents first, then install Avaya Communication Manager on and configure the media server and verify its operation.

This section covers the following tasks:

- Configuring the SNMP modules in the UPS on page 34
- Configuring the SNMP subagent in the Avaya Ethernet switch (if used) on page 37
- Configuring the media server on page 39
- Configuring the maintenance adapter on page 52

Configuring the SNMP modules in the UPS

NOTE:
These instruction apply only if using a new, Avaya-supplied uninterruptible power supply (UPS) with a simple network management protocol (SNMP) module. Do not use these procedures to set traps on a non-Avaya-provided UPS.

NOTE:
Because the SNMP module is manufactured by a third party, we do not know which brand, model, or firmware load the factory is shipping. Therefore, we cannot provide specific instructions in this document on how to connect to and configure the SNMP module. Refer to the documentation that comes with the SNMP module.

Make sure the CAT5 straight-through cables are connected from the UPSs' SNMP modules to the next available port on the customer's network. For a connectivity guide, see *Quick Start Hardware Installation: Avaya S8500 Media Server* (555-245-701). Make sure you are plugged into the correct port on the SNMP module.

The SNMP module in the UPS must be administered so it reports alarms to the media server when the hardware experiences problems. The module reports the loss of commercial power and the depletion of battery resources.

The SNMP module requires a unique IP address, which can be a customer-provided one or the Avaya-provided default one. At a minimum, the following items need to be configured:

- IP address
- Default gateway IP address
- Subnet mask
- Community name strings (get, set, trap)

NOTE:
For the SNMP module to properly report alarms, the IP address for the UPS must also be configured in the media server.

See Setting selected traps (alarming) on page 36 for information on which traps to set.

See the local configuration section of the User's Guide that comes with the SNMP module for the default password and the configuration commands.

To administer the SNMP modules:

1. Make sure the UPS is plugged into a nonswitched electrical outlet.
2. Connect the services laptop computer (RS-232 serial port) to the DB-9 connector on the back of the SNMP module for UPS 1 using the DB-9 to DB-9 serial cable supplied with the SNMP module.

   NOTE:
   Avaya Terminal Emulation and HyperTerminal are supported terminal emulation applications.

3. On the services laptop open a VT-100 terminal emulation session.

4 Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control

5 Follow the instructions in the User's Guide.

6 Set the following parameters:
   - IP address and subnet mask of the UPS. (defaults are 198.152.254.239, 255.255.255.0.)
   - IP address of the trap receiver. (default is 198.152.254.200)
   - Default Gateway address of the UPS is 198.152.254.201.

     NOTE:
     If a Network Management System (NMS) is going to monitor the UPS, coordinate the assignment of community names with the network administrator. If an NMS is not going to monitor the UPS, set the community names to unique string values.

   - SNMP community string for Get, Set, and Trap.

     SECURITY ALERT:
     The **Get** and **Set**, community name strings are generally configured with default values of **Public** and **Private,** respectively. These community name strings function as passwords for their respective SNMP operation. It is always a good idea to change these community name strings to something other than the default values. If a NMS is in operation on the network, whatever these values are changed to must be coordinated with its administrator. If the defaults are left administered this could create a **serious security issue.** For example, the default Set community name string, with its widely known value of Private, could be used to shut down power to the UPS loads via an SNMP message.

7 When completed, disconnect the services laptop computer from the UPS.

8 Connect one end of a CAT5 cable to the RJ45 connector on the UPS's SNMP module and the other end to the next available port on the Ethernet switch for the control network.

Single control network

If a single control network, use the following address and cable connection information:

- UPS IP address / Subnet mask = **198.152.255.238 / 255.255.255.0**
- Default Gateway IP address = **198.152.254.202**
- Host Table trap receiver IP address = **198.152.254.202**
- Local network administrator supplied information as required for Get and Set community name strings.

Setting selected traps (alarming)

The default is to set all traps, which may result in large log entries. Therefore, only set the following traps. See the User's Guide that comes with the SNMP module for the menus and commands for setting these traps.

- UPS on Battery—Indicates AC fail with pending shutdown based on battery reserve available
- UPS in Bypass—Failure either Failed UPS or overload
- Replace battery—Failure of periodic (28-day) battery test indicating battery needs to be replaced.

Configuring the SNMP subagent in the Avaya Ethernet switch (if used)

NOTE:
These instruction apply only if using a new, Avaya-supplied Avaya Ethernet switch. Do not use these procedures to set traps on a non-Avaya-provided Ethernet switch.

NOTE:
We do not know which Avaya Ethernet switch model or firmware load the factory is shipping. Therefore, we cannot provide specific instructions in this document on how to configure the SNMP subagent. Refer to the documentation that comes with the switch.

The simple network management protocol (SNMP) subagent in the Avaya Ethernet switch must be administered so it can report alarms to the media server when the hardware experiences problems.

Each Avaya Ethernet switch requires a unique IP address, which can be a customer-provided one or the Avaya-provided default one. At a minimum, the following items need to be configured:

- IP address
- Subnet mask
- Trap receiver IP address
- Community string (get, set, trap)
  - — Spanning tree
  - — Ethernet port speed (if applicable)

NOTE:
For the Ethernet switch to properly report alarms, the IP address(es) for the Ethernet switch(es) must also be configured in the media servers.

See the Basic Configuration section of the Quick Start Guide and the documentation CD that comes with the Ethernet switch for the default user ID, password, and configuration commands.

To administer the Ethernet switch(es):

1. Plug the Ethernet switch power cord into the back of the switch and the back of a UPS.
2. Connect the services laptop computer (RS-232 serial port) to the port labeled Console on the front of Ethernet switch 1 (CNA) using the flat cable supplied with the Avaya Ethernet switch.
3. On the services laptop open a VT-100 terminal emulation session.
4. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
5. Follow the instructions in the Quick Start Guide

6 Set the following parameters:

- IP address and subnet mask of the Ethernet switch (defaults are 198.152.254.240, 255.255.0.0.)
- IP address of the trap receiver. (default is 198.152.254.200)
- SNMP community string for Get, Set, and Trap. (See the section on SNMP commands on the documentation CD that comes with the Avaya Ethernet switch.)

SECURITY ALERT:

The **Get** and **Set**, community name strings are generally configured with default values of **Public** and **Private,** respectively. These community name strings function as passwords for their respective SNMP operation. It is always a good idea to change these community name strings to something other than the default values. If a Network Management Station (NMS) is in operation on the network, whatever these strings are changed to must be communicated to the NMS administrator. If the defaults are left administered this could create a **serious security issue.** For example, the default Set community name string, with its widely known value of Private, could be used to reconfigure the Ethernet switch via SNMP message.

7 Set spanning-tree to disabled (default is enabled)

Use the command **set spanning disable**.

8 If IP Connect, make sure all appropriate ports on the Ethernet switch are locked to 100 speed using full duplex.

9 When completed, disconnect the services laptop computer from the Ethernet switch.

10 If two Ethernet switches are present for CNA, repeat steps 1 through 7 for the second switch.

Configuring the media server

A new media server comes with a blank hard drive and a bootable CD-ROM with Linux operating system and Release 2.1 of Avaya Communication Manager on it.

Use the instructions in *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-701)to install the media server in the data rack. After installing the media server, you must install the software from the CD onto the hard drive.

This section covers the following tasks:

- Clearing the ARP cache on the laptop on page 39
- Disabling the RSA loader watchdog on page 40
- Powering up the media server on page 41
- Accessing the media server on page 41
- Setting up Telnet on page 41
- Installing Avaya Communication Manager on page 42
- Using the Installation Wizard on page 43
- Configuring the maintenance adapter on page 52
- Verifying media server connection to the customer's LAN (if provided) on page 45
- Configuring the modem on page 46
- Checking LED activity on the optional dual NIC on page 48
- Disconnecting from the media server on page 48

NOTE:
Make sure you have the filled-out *Electronic Preinstallation Worksheet* (EPW) before beginning this process.

NOTE:
Make sure your networking and Web browser settings are correct. See Appendix A, Network configuration on page 100.

Clearing the ARP cache on the laptop

NOTE:
Depending on your laptop computer's operating system (generally Windows 2000), you may need to clear the Address Resolution Protocol (ARP) cache before entering a new IP address. If you enter an IP address, and your computer cannot connect, then you may need to clear the cache.

1. On your laptop computer click **Start > Run** to open the Run dialog box.
2. Type **command** and press **Enter** to open a MS-DOS Command Line window.
3. Type **arp -d 192.11.13.6** and press **Enter** to clear the Address Resolution Protocol (ARP) cache in the laptop. This command responds with one of the following:
   - The command line prompt when the cache has been cleared.

- The phrase: `The specified entry was not found.`

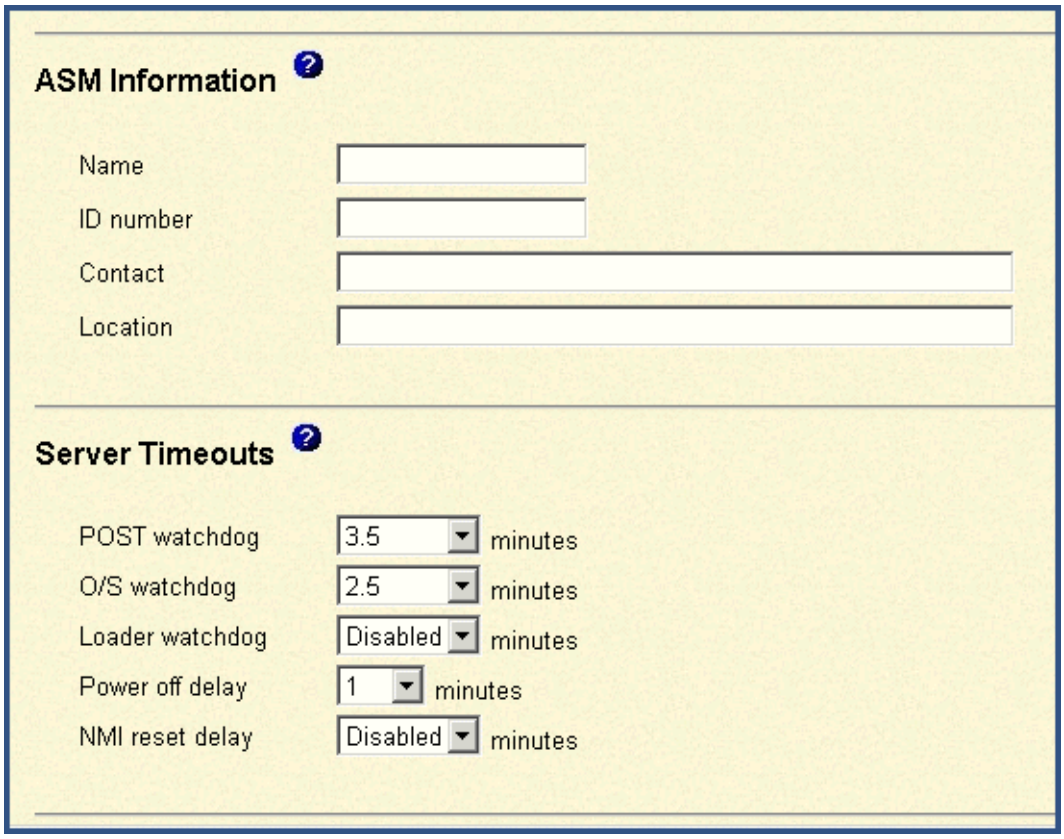
  This is returned when the specified IP address does not currently appear in the ARP cache.

Disabling the RSA loader watchdog

NOTE:
Perform this procedure to prevent the Remote Supervisor Adapter (RSA) from resetting the media server during the installation process. Failure to do this procedure may mean the media server resets and you have to start the installation process at the beginning.

NOTE:
We recommend that for RSA you use an external power source on a different circuit from the Avaya S8500 Media Server.

1. Make sure the cord is connected from the power connector on the RSA to a UPS or nonswitched electrical outlet.
2. Connect the laptop to the Ethernet port on the RSA using a crossconnect cable.
3. Open a browser.
4. In the **Address** field type **192.11.13.6** and press **Enter**.
5. Log on as **craft**, using the password **passw0rd** (with a zero).
6. Under ASM Control click **System Settings**.



7 In the **Loader watchdog** field, select **Disabled**.

8 Scroll down and click **Save**.

9 Clear the ARP cache on the laptop. See Clearing the ARP cache on the laptop on page 39

Powering up the media server

1 Connect the AC power cord to the media server and to the UPS or a nonswitched outlet to power it up. If it does not power up, press the white power control button on the front of the media server.

Accessing the media server

NOTE:
You must place the CD in the drive immediately.

1 Connect the laptop to the services port (port 2 [Eth1]) on the back of the media server using a crossconnect cable.

2 Place the CD with Avaya Communication Manager in the CD-ROM drive on the media server.

3 Wait at least 3 minutes after powering up before starting a Telnet session to access the information on the CD.

Setting up Telnet

NOTE:
Use a telnet session to access the information on the CD.

The Microsoft Telnet application may be set to send a carriage return (CR) and line feed (LF) each time you press Enter. The installation program sees this as 2 key presses. If running Windows 2000/XP, you need to correct this before you copy the Remaster Program to the hard drive.

1 Click **Start** > **Run** to open the Run dialog box.

2 Type **telnet** and press **Enter** to open a Microsoft Telnet session.

3 Type **display** and press **Enter** to see the current settings. If message says

```
Sending only CR
```

then close the dialog box.

If message says

```
Sending both CR & LF
```

then continue with step 4.

4 Type **unset crlf** and press **Enter**.

5 Type **display** and press **Enter** to verify that the settings changed. The message says

```
Sending only CR
```

6 Close the dialog box.

NOTE:

Installing Avaya Communication Manager

NOTE:
Use a telnet session to access the information on the CD.

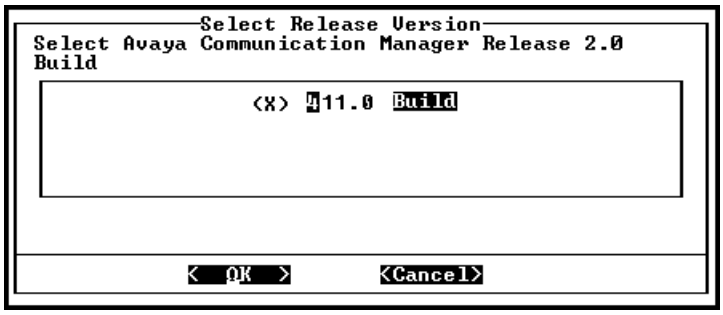
1 Type **telnet 192.11.13.6** and press **Enter** to view the first screen.

What do you want to do?
The hard drive is currently Partitioned
Choose One
(X) Install Install or Upgrade MV Software
( ) Shell Boot to Rescue Bash Shell
( ) Quit Reboot the server
< OK >

NOTE:
To navigate on these screens, use the arrow keys to move to an option, then press the space bar to select the option. Press **Enter** to submit the screen.

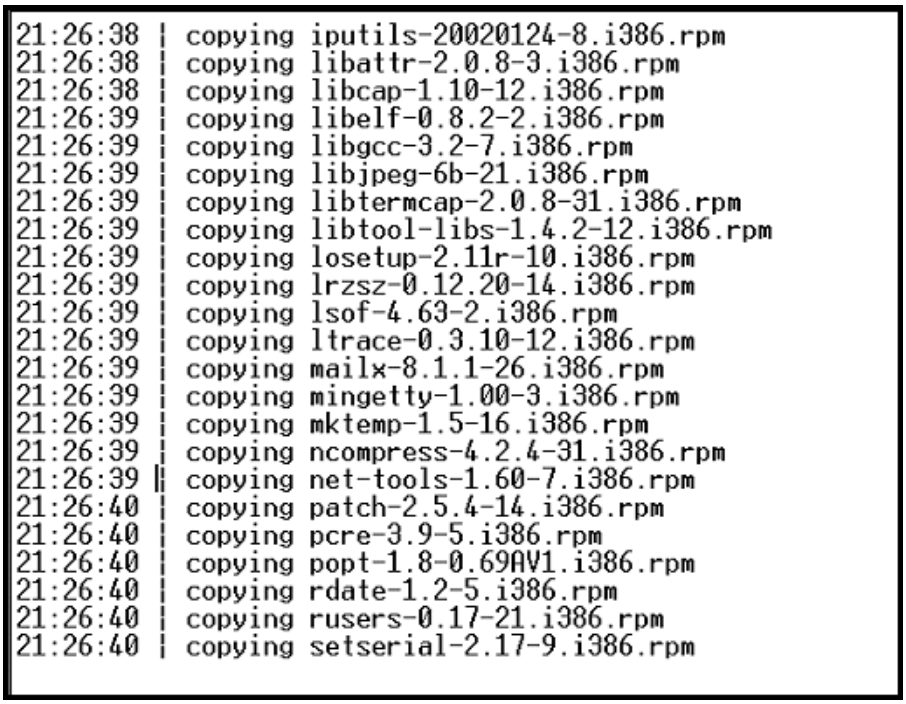
2 Select **Install**, make sure OK is highlighted, and press **Enter**.

3 Select **<Yes>** and press **Enter**.



4 Select **<OK>** and press **Enter** to partition the hard drive and reformat the partitions

Once the drive is properly configured, the program begins the installation process and reports the progress.


21:26:38 | copying iputils-20020124-8.i386.rpm
21:26:38 | copying libattr-2.0.8-3.i386.rpm
21:26:38 | copying libcap-1.10-12.i386.rpm
21:26:39 | copying libelf-0.8.2-2.i386.rpm
21:26:39 | copying libgcc-3.2-7.i386.rpm
21:26:39 | copying libjpeg-6b-21.i386.rpm
21:26:39 | copying libtermcap-2.0.8-31.i386.rpm
21:26:39 | copying libtool-libs-1.4.2-12.i386.rpm
21:26:39 | copying losetup-2.11r-10.i386.rpm
21:26:39 | copying lrzsz-0.12.20-14.i386.rpm
21:26:39 | copying lsof-4.63-2.i386.rpm
21:26:39 | copying ltrace-0.3.10-12.i386.rpm
21:26:39 | copying mailx-8.1.1-26.i386.rpm
21:26:39 | copying mingetty-1.00-3.i386.rpm
21:26:39 | copying mktemp-1.5-16.i386.rpm
21:26:39 | copying ncompress-4.2.4-31.i386.rpm
21:26:39 | copying net-tools-1.60-7.i386.rpm
21:26:40 | copying patch-2.5.4-14.i386.rpm
21:26:40 | copying pcre-3.9-5.i386.rpm
21:26:40 | copying popt-1.8-0.69AV1.i386.rpm
21:26:40 | copying rdate-1.2-5.i386.rpm
21:26:40 | copying rusers-0.17-21.i386.rpm
21:26:40 | copying setserial-2.17-9.i386.rpm

These processes can take up to 20 minutes. When the media server is ready to reboot, the CD-ROM drive drawer opens. You must remove the CD from the drive at this time.

The reboot may take up to 3 minutes. The telnet session drops automatically.

Using the Installation Wizard

You can configure the media server and install the license, Avaya authentication files, and software updates automatically using the Avaya Installation Wizard. You can do it two ways:

- You can import the data from the filled-out *Electronic Preinstallation Worksheet* (EPW).
- You can also type in the information manually using the filled-out EPW as a guide.

NOTE:
You can install the license file without being physically connected to the reference IPSI. However, you have only 30 minutes before it checks the serial number on the IPSI. To get another 30 minutes, you can restart the clock by restarting the media server. In a SAT session, type **reset system 1**.

1 Launch the Web browser.

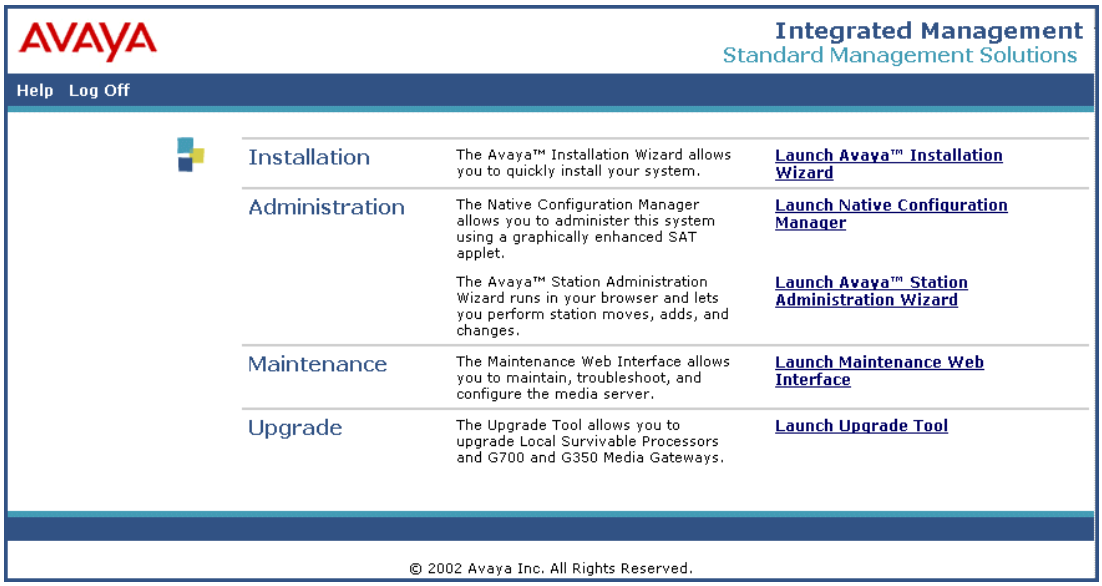
2 In the **Address** field, type **192.11.13.6** and press **Enter** to bring up the login Web page.

NOTE:
The first time you attempt to log in, you get a Web page asking you to install a security certificate. Follow the instructions for your particular browser to accept the certificate. You can also install the certificate on your services laptop computer by following the instructions in your browser's online help.

3 Log in as **craft** and use the initial craft password.

4 When asked **Do you want to suppress alarms?**, select **Yes**.

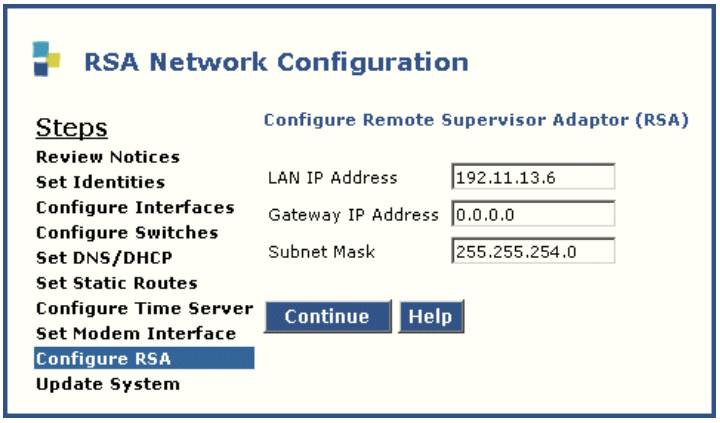
NOTE:
On the initial Web page, some items may not appear at first. These include Launch Avaya Station Administration Wizard in the Administration section and the Upgrade section including Launch Upgrade Tool.


AVAYA
Integrated Management
Standard Management Solutions
Help Log Off
Installation
The Avaya™ Installation Wizard allows you to quickly install your system.
Launch Avaya™ Installation Wizard
Administration
The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.
Launch Native Configuration Manager
The Avaya™ Station Administration Wizard runs in your browser and lets you perform station moves, adds, and changes.
Launch Avaya™ Station Administration Wizard
Maintenance
The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.
Launch Maintenance Web Interface
Upgrade
The Upgrade Tool allows you to upgrade Local Survivable Processors and G700 and G350 Media Gateways.
Launch Upgrade Tool
© 2002 Avaya Inc. All Rights Reserved.

5 Click **Launch Avaya Installation Wizard**.

6 Follow the prompts, using Help on each page for more information.

The Configure RSA page is the next to last page in the AIW configuration process.



7 Verify the IP information for the RSA card has retrieved the data from the EPW. If the information is not there, manually complete all fields.

- **LAN IP Address** field - **192.11.13.6**
- **Gateway IP Address** field - **0.0.0.0**
- **Subnet Mask** field - **255.255.254.0**

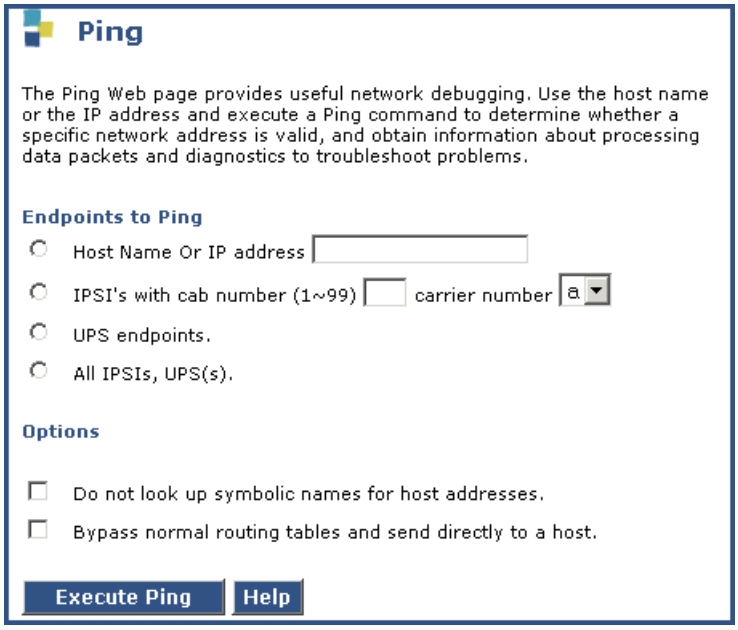
The above information configures the RSA for the crossconnect cable.

To finish configuring the maintenance adapter, see Configuring the maintenance adapter on page 52.

Verifying media server connection to the customer's LAN (if provided)

To verify media server connection to the customer's LAN:

1 Under Diagnostics, click **Ping**.


Ping
The Ping Web page provides useful network debugging. Use the host name or the IP address and execute a Ping command to determine whether a specific network address is valid, and obtain information about processing data packets and diagnostics to troubleshoot problems.
Endpoints to Ping
Host Name Or IP address
IPSI's with cab number (1~99)
carrier number
a
UPS endpoints.
All IPSIs, UPS(s).
Options
Do not look up symbolic names for host addresses.
Bypass normal routing tables and send directly to a host.
Execute Ping
Help

2. Select "Host Name Or IP Address" and type in the IP address of a computer on the network.
3. Click **Execute Ping**.
4. Verify that the ping was successful, indicating that the media server is connected to the customer's network.
5. If DNS is administered, type in the host name of a computer on the network.
6. Click **Execute Ping**.
7. Verify that the ping was successful, indicating that DNS is working.

If available, have a customer representative do the following test from a computer on the network:

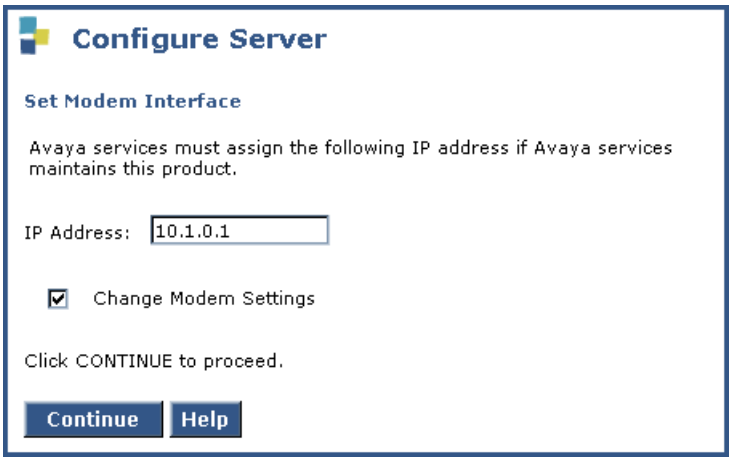
8. Click **Start > Run** to open the ***Run*** dialog box.
9. Type **command** and click **OK** to open an MS-DOS command window.
10. Type **ping *serveripaddress*** and click **OK**, where ***serveripaddress*** is the IP address of the media server.
11. Verify that the ping was successful.
12. If DNS is administered, type **ping *servername*** and press **Enter**, where ***servername*** is the host name of the media server.
13. Verify that the ping was successful.

Configuring the modem

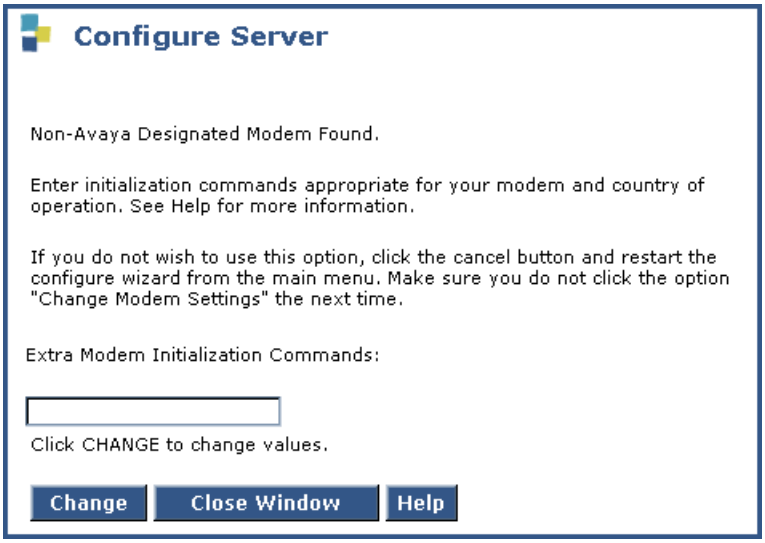
1. Under Server Configuration click **Configure Server**.
2. Click through until you get to the ***Specify how you want to use this wizard*** page

3. Select **Configure individual services** and click **Continue**.

4 In the left menu click **Set Modem Interface**.



5 Select the **Change Modem Setting** and click **Continue**.


Configure Server
Non-Avaya Designated Modem Found.
Enter initialization commands appropriate for your modem and country of operation. See Help for more information.
If you do not wish to use this option, click the cancel button and restart the configure wizard from the main menu. Make sure you do not click the option "Change Modem Settings" the next time.
Extra Modem Initialization Commands:
Click CHANGE to change values.
Change
Close Window
Help

6 In the **AT String** field, type the initialization commands appropriate for your modem and country of operation. Click Help for guidance on what to enter.

For example, to change the country code to Japan, type **AT%T19,0,10**.

7 Click **Change**.

The system responds with a message indicating a successfully added modem route.

8 Click **Close Window**.

Checking LED activity on the optional dual NIC

When the media server is in service, check the LEDs on each port of the dual network interface card (NIC) to make sure there is a connection (left LED) and activity (right LED). See Figure 1, S8500 rear panel dual NIC LEDs, on page 48.

Figure 1: S8500 rear panel dual NIC LEDs

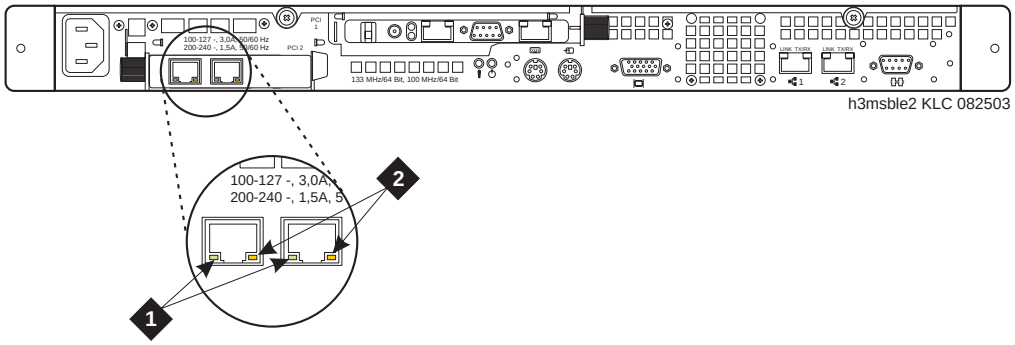


Figure notes

1 Network activity LED (TX/RX)

2 Connection rate:

- Off: a 10 BASE-T active link.
- GREEN: a 100 BASE-T active link.
- ORANGE: a 1000 BASE-T active link.

Disconnecting from the media server

1 Unplug the crossconnect cable from the services port on the back of the media server.

Configuring the dual NIC

This section describes the tasks required to configure the optional dual network interface card (NIC) on the Avaya S8500 Media Server. The tasks include:

- Configuring the NIC on page 49
- Configuring the NIC on page 49
- Testing connectivity to customer's network on page 50

Configuring the NIC

1. Under Server Configuration click **Configure Server**.
2. Click **Continue** through the review notices until you get to the ***Specify how you want to use this Wizard*** page.

3. Select **Configure Individual Services** and click **Continue**.
4. Select **Set Identities** and click **Continue**.
5. Assign Ethernet port functions using the drop-down menus for the following fields:
   - **Control Network A**: [default: Ethernet 0]
   - **Services Port**: [default: Ethernet 1]
   - **Corporate LAN**: [default: Ethernet 0]. Set this field to **Ethernet 2** to have the IPSI control on a dedicated, separate Ethernet port.
   - **Unused**
6. Click **Continue**.
7. Fill in the following information for Ethernet 2:
   - IP address
   - Gateway
   - Subnet mask
   - Speed

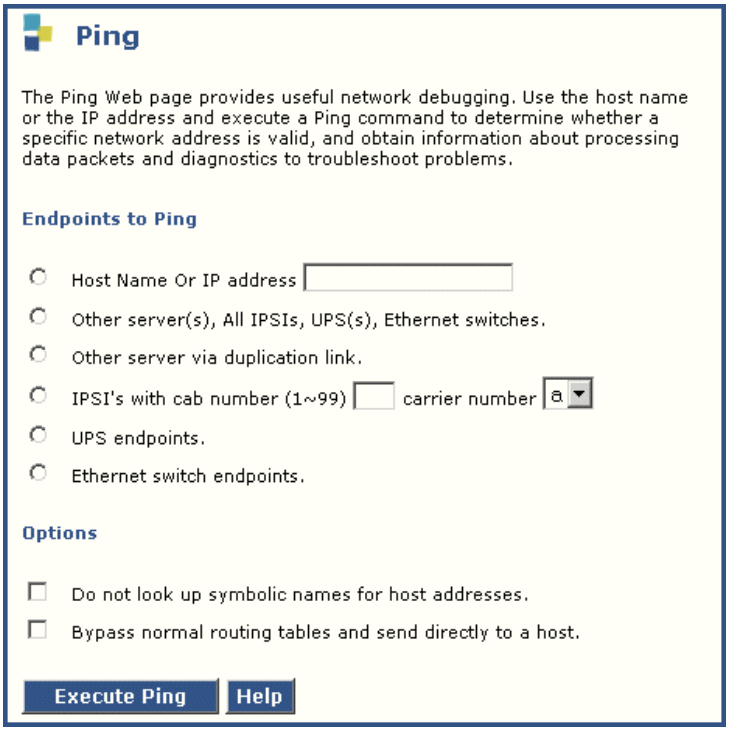
8. Verify with the customer's network administrator that the LAN hardware supports 802.1q priority tagging. If supported, select "VLAN 802.1q priority tagging."
9. Click **Change**. The status of the configuration update appears in the window.

   When the update completes, the following message appears:

   `Successfully configured ethernet interfaces.`

Testing connectivity to customer's network

1. Under Diagnostics click **Ping**.


Ping
The Ping Web page provides useful network debugging. Use the host name or the IP address and execute a Ping command to determine whether a specific network address is valid, and obtain information about processing data packets and diagnostics to troubleshoot problems.
Endpoints to Ping
Host Name Or IP address
Other server(s), All IPSIs, UPS(s), Ethernet switches.
Other server via duplication link.
IPSI's with cab number (1~99)
carrier number
a
UPS endpoints.
Ethernet switch endpoints.
Options
Do not look up symbolic names for host addresses.
Bypass normal routing tables and send directly to a host.
Execute Ping
Help

2. Select **Host Name or IP address** and type in the IP address of a computer on the network.
3. Click **Execute Ping**.
4. Verify that the ping was successful, indicating that the media server is connected to the customer's network.
5. If DNS is administered, type in the host name of a computer on the network.
6. Click **Execute Ping**.
7. Verify that the ping was successful, indicating that DNS is working.

If available, have a customer representative do the following test from a computer on their network:

8. Click **Start** > **Run** to open the ***Run*** dialog box.
9. Type **command** and click **OK** to open an MS-DOS command window.
10. Type **ping *serveripaddress*** and click **OK**, where ***serveripaddress*** is the IP address of media server.
11. Verify that the ping was successful.

12 If DNS is administered, type **ping *servername*** and press **Enter**, where ***servername*** is the host name of media server.

13 Verify that the ping was successful.

Configuring the maintenance adapter

This section describes the steps required to configure the maintenance adapter, which for this release is the Remote Supervisor Adapter (RSA), on the Avaya S8500 Media Server. These tasks include:

- Connecting and logging into the adapter on page 52.
- Setting auto answer on the RSA on page 59.
- Enabling the RSA loader watchdog on page 60.
- Logging off the RSA on page 60.

Connecting and logging into the adapter

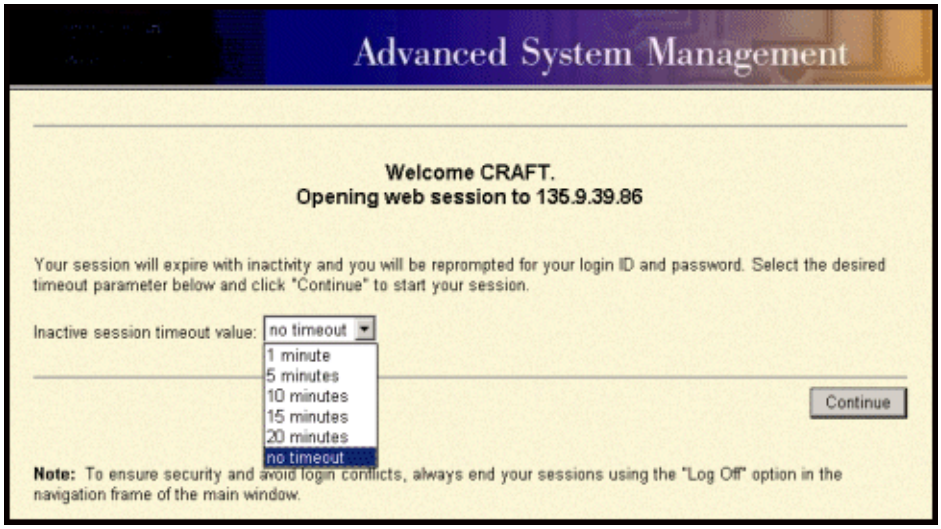
NOTE:
After completing some of the following steps you are prompted to restart ASM. Do not restart ASM at this time. You will be reminded to restart the ASM once all the configuration steps are completed.

1 Connect the services laptop to the Ethernet port on the RSA using a crossconnect cable.

1 Launch the Web browser.

2 In the **Address** field type **192.11.13.6** and press **Enter** to bring up the ***Enter Network Password*** page.

3 Log on as **craft,** using the initial craft or unique customer password.


Advanced System Management
Welcome CRAFT.
Opening web session to 135.9.39.86
Your session will expire with inactivity and you will be reprompted for your login ID and password. Select the desired timeout parameter below and click "Continue" to start your session.
Inactive session timeout value:
no timeout
1 minute
5 minutes
10 minutes
15 minutes
20 minutes
no timeout
Continue
Note: To ensure security and avoid login conflicts, always end your sessions using the "Log Off" option in the navigation frame of the main window.

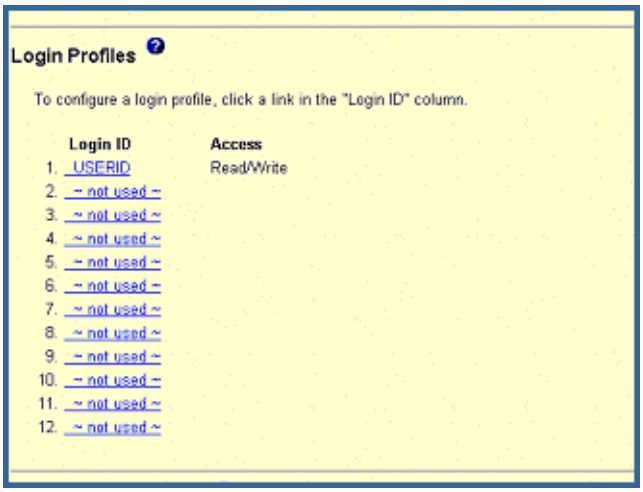
4 From the **Inactive session time value** field, click **no timeout**, which allows 60 minutes of use before disconnecting.

NOTE:
If the session times out unexpectedly, click **Start New Session** and **Refresh**.

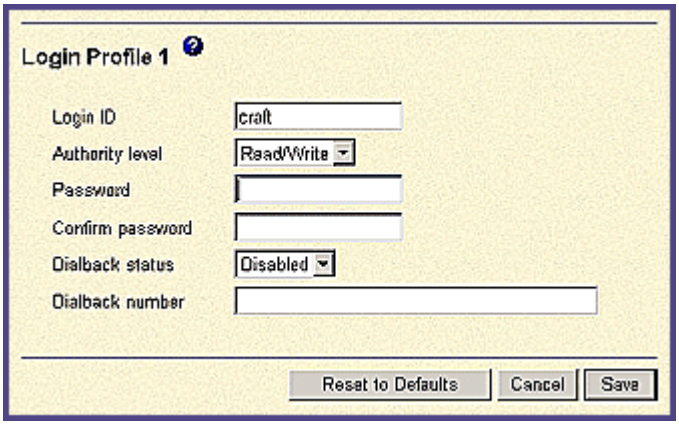
5 Click **Continue**.

Adding login IDs and passwords

1 Under **ASM Control** click **Login Profiles**.


Login Profiles
To configure a login profile, click a link in the "Login ID" column.
Login ID
Access
1. USERID
Read/Write
2. ~ not used ~
3. ~ not used ~
4. ~ not used ~
5. ~ not used ~
6. ~ not used ~
7. ~ not used ~
8. ~ not used ~
9. ~ not used ~
10. ~ not used ~
11. ~ not used ~
12. ~ not used ~

2 Under the **Login ID** column, click the first nonconfigured line (~not used~).



3 Fill in the following fields:

- **Login ID:** type in the new user ID.
- **Authority level:** select **Read/Write**.
- **Password:** type in the new password.
- **Confirm Password:** retype the new password.

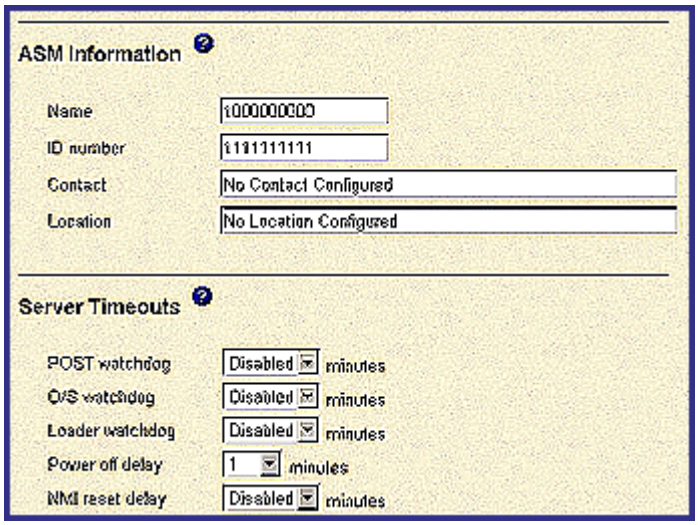
4 Click **Save** to return to the Login Profiles page.

5 Repeat steps 2 through 4 for each new login.

6 Scroll down to the bottom and click **Save**.

Configuring Advanced System Management

1 Under **ASM Control** click **System Settings**.



2 Fill in the following fields:

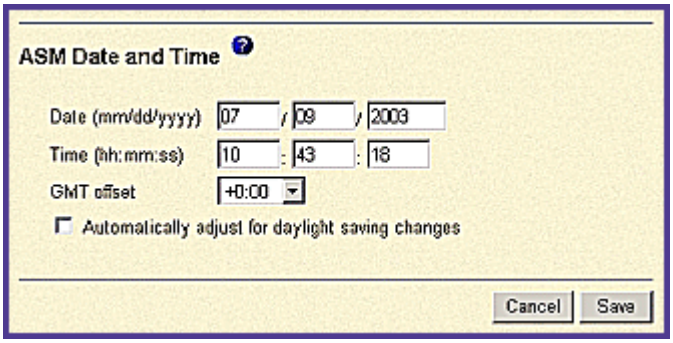
- **Name:** type in the product ID number.

  The product ID number is the same as that for the media server. A different product ID number can be used if alarming is going to some place other than Avaya.

- **Contact:** type in the contact information.
- **Location:** type in the location information.

3 Scroll down to the bottom of the page and click **Save**.

4 Scroll down to **ASM Date and Time** and click **Set ASM Date and Time**.



5 Type the current date and time in the correct fields.

6 In the **GMT offset** field select the Greenwich Mean Time offset for your region. For example, Denver, Colorado, would be - 7:00 for MST.

7 Select "Automatically adjust for daylight savings time changes" if daylight savings is used in your area.

8 Click **Save** to return to the ***System Settings*** page.

9 Scroll down to the bottom of the page and click **Save**.

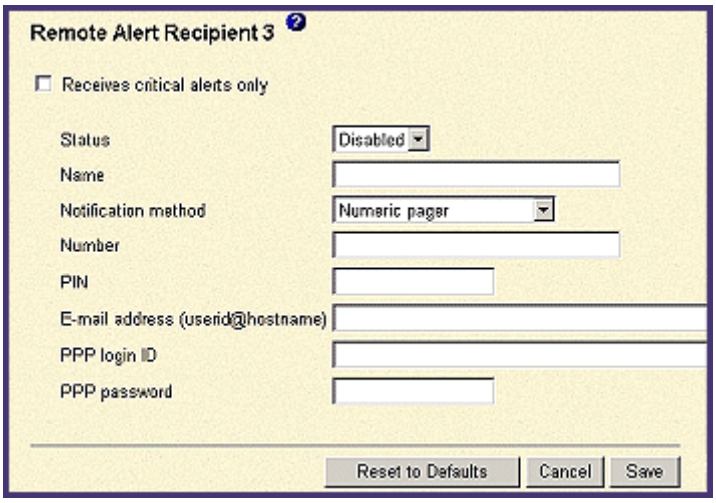
Setting alarms

Although the configuration for the remote alarming is done in one section, you need to see other panes to complete the configuration before you test it. For more detailed information, see the *Avaya Remote Supervisor Adapter Users' Guide* (555-245-702).

1 Under **ASM Control** click **Alerts**.

Remote Alert Recipients
To configure a remote alert recipient, click a link in the "Name" column.
Name
Notification Method
Status
1. Chintan PC
IBM Director over modem
Receives all alerts
2. Pstio
SNMP over LAN
Receives all alerts
3. ~ not used ~
4. ~ not used ~
5. ~ not used ~
6. ~ not used ~
7. ~ not used ~
8. ~ not used ~
9. ~ not used ~
10. ~ not used ~
11. ~ not used ~

2 Under the **Name** column click on the first nonconfigured line (~not used~).



NOTE:
Do not select the **Receives Critical Alerts Only**.

3 Fill in the following fields:

- **Status**: select **Enabled**.
- **Name**: Type in **Avaya services** or **INADS.**
- **Notification method**: Select one of the following from the drop-down menu:
  - To send alerts to INADS over modem, select **IBM Director over Modem**.
  - To send alerts to INADS over SNMP, select **SNMP over LAN**.

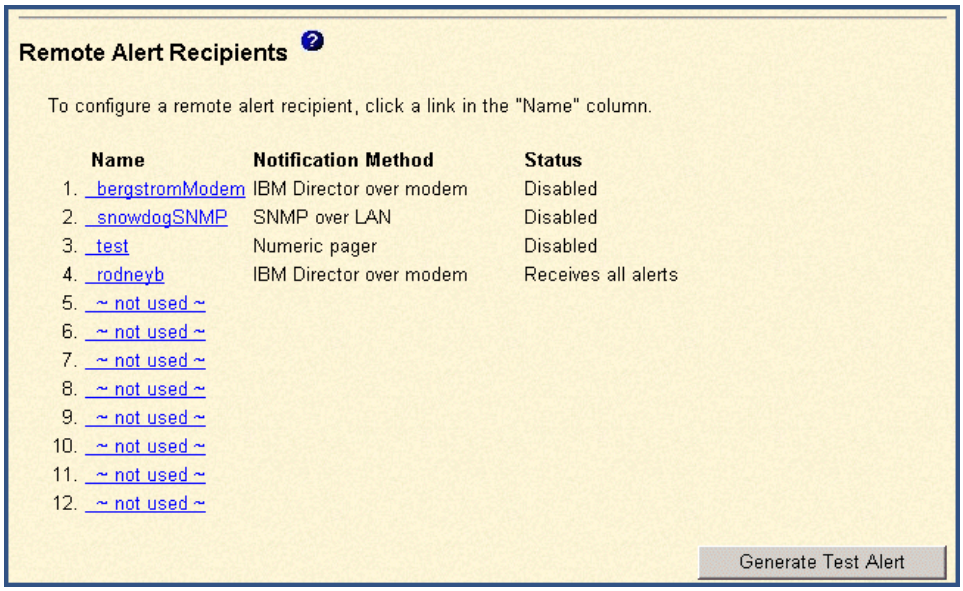
- **Number**:
  - If you select **IBM Director over Modem**, type in **918666885928** (if a direct line, you do not need the **9**).
  - If you select **SNMP over LAN**, type in the Avaya IP address or Avaya hostname that will receive the SNMP alerts. Additional administration must be completed in the **Network Protocols** section before **SNMP over LAN** is used.

4 Click **Save** to return to the Remote Alert Recipients page.

This is the only part you must fill out in the **Alerts** section. Keep the remaining fields as Avaya default settings.

5 Once all the Alerts configuration is completed, click **Alerts**.

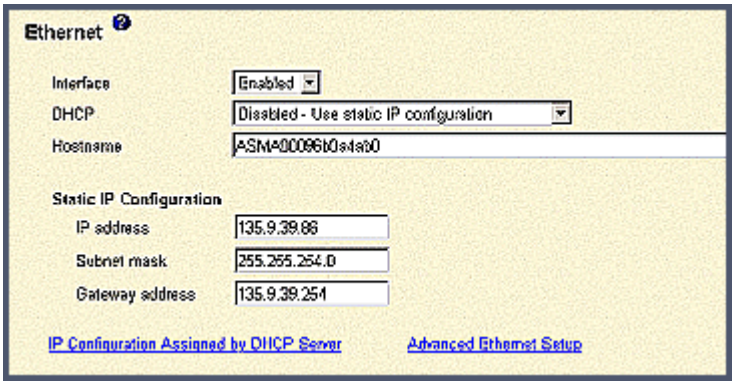
6 Click **Generate Test Alert**.



Verifying network interfaces

The network interfaces are populated with information from the Avaya Installation Wizard when configuring the media server. Verify that the fields were populated.

1. Under **ASM Control** click **Network Interfaces**.



2. Verify that all the fields are filled in and are correct.

Restart ASM

1. Under **ASM Control** click **Restart ASM** to reboot.

Backing up the configuration

Once the configuration is complete, you can back up the RSA administration changes. In case something happens to the RSA, the settings can be restored easily. A copy of the ASM backup can be stored on the customer's network. Because there is not connection to the customer's network from the RSA, you must first save the file to the laptop computer, then back the file up to the customer's network.

NOTE:
Backing up this way is not always successful. If you have a problem, follow normal escalation procedures.

You must have a login ID and password for the customer's network. You can use the backup copy to restore the RSA configuration in the event of damage or corruption.

1. If not logged in, log into the RSA.
2. Under ASM Control click **Configuration File**.
3. In the **Backup ASM Configuration** section click **View the current configuration summary**.
4. Verify that these are the settings that you want to save, then click **Close**.

If the settings are not correct, go to the respective areas and update the information. See Table 1, Updating the configuration summary, on page 58. To review system defaults, see Avaya RSA defaults on page 107.

Table 1: Updating the configuration summary

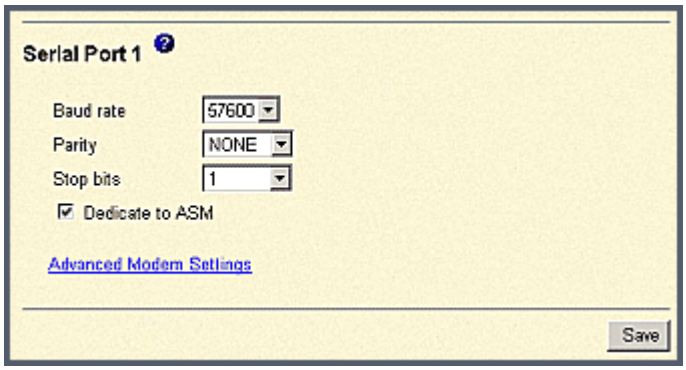
Configuration summary item	Where to update information
ASM Information	System Settings
Server Timeouts	System Settings
ASM Date and Time	System Setting
Scheduled Power On	**Power/Restart** > **Server Power** / **Restart Control** > **Power on at Specified Time**
Remote Control Keys	Remote Control Keys
Login Profiles	Login Profiles
Global Login Settings	Login Profile
Remote Alert Recipients	Alerts
Alert Forwarding	Alerts
Global Remote Alert Settings	Alerts
Monitored Alerts	Alerts
Monitored Local Events	Alerts
Serial Port	Serial Port
Modem Settings	**Serial Port** > **Advanced Modem Settings**
Ethernet	Network Interfaces
Advanced Ether Setup	**Network Interfaces** > **Advanced Ethernet Setup**
PPP over Serial Port	Network Interfaces
SNMP	Network Protocols
DNS	Network Protocols
SMTP	Network Protocols

5. In the **Backup ASM Configuration** section click **Backup**.
6. Type in a name for the backup file and choose a location on the services laptop to store the backup file.
7. Select **Save this file to disk** and then **OK**.
8. To back up the file to the customer's network, connect directly to a port on the customer's network.
9. Click **Start** > **Run** to open the ***Run*** dialog box.
10. Type **ping *IPaddress***, where ***IPaddress*** is the address for the server you are backing the files up to, is and press **Enter** to verify that you can access the server from the laptop.
11. Use FTP to move the file from the services laptop to the customer's network.

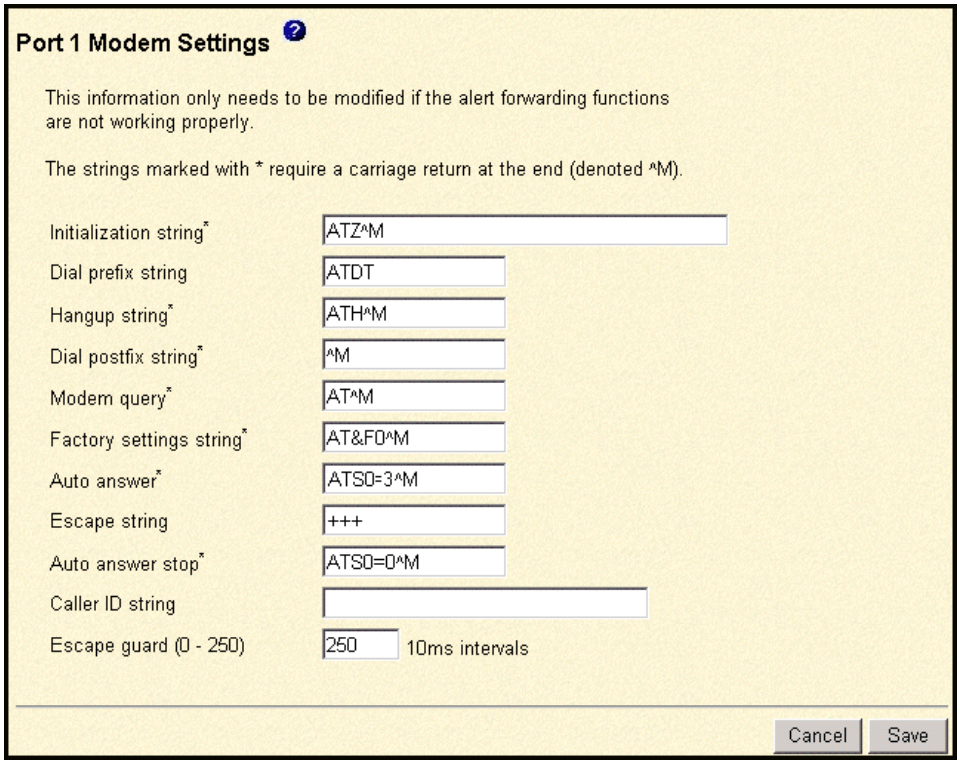
Setting auto answer on the RSA

You can determine how many times the phone rings before the RSA card answers the call.

1 Under **ASM Control** click **Serial Port**.



2 In the Serial Port section, click **Advanced Modem Settings**.



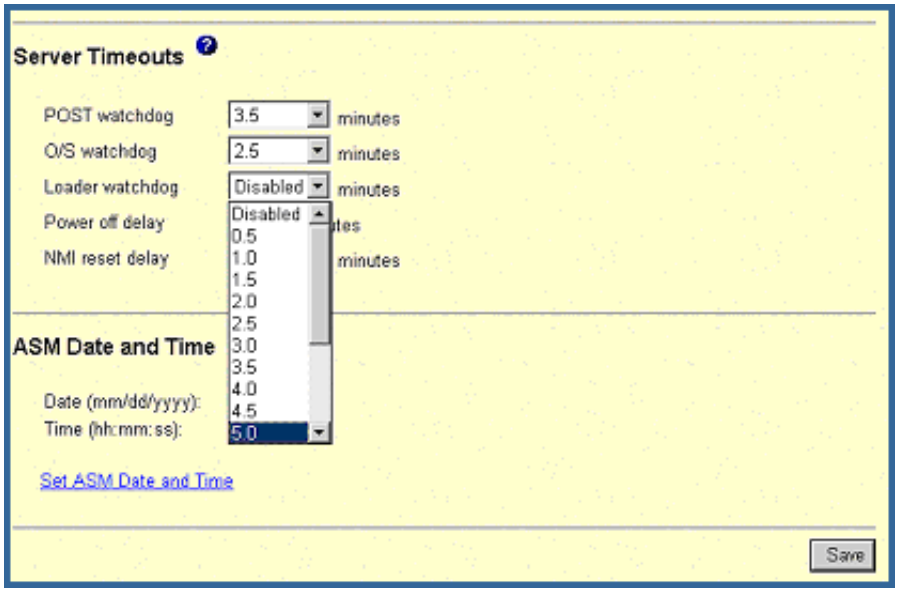
3 In the **Auto Answer** field set to **ATSO=3^M**.

4 Click **Save**.

Enabling the RSA loader watchdog

NOTE:
If the loader watchdog was disabled earlier, you must enable it.

1. Log on as **craft**, using the initial craft or unique customer password.
2. Under **ASM Control** click **System Settings**.



3. In the Loader watchdog field, click **5.0** (minutes).
4. Click **Save**.

Logging off the RSA

1. From the left pane, select **Log Off**.
2. In the confirmation window, click **Yes**.

3 Connecting to the IPSIs

NOTE:
The media gateways must be installed, connected to each other, and powered up.

This chapter covers the following tasks:

- Programming the IPSI circuit packs on page 61
- Verifying that IPSIs are translated on page 66
- Verifying connectivity to media server on page 66
- Upgrading IPSI firmware version (if necessary) on page 67
- Enabling control of IPSIs on page 67
- Verifying license status on page 67
- Reusing a TN2312AP/BP circuit pack on page 68

NOTE:
At a minimum you must program the reference IPSI and connect to it to avoid going into No License Mode.

NOTE:
Once the IPSIs are connected to the control network, they may alarm if the firmware is not the most current. The alarm automatically goes away once the IPSI firmware is upgraded.

IP Connect: Connect one end of the GREEN CAT5 straight-through cable to the IPSI adapter on the back of media gateway in position A. The other end is connected to the next available port on the customer's network. If not already connected, connect it.

Direct connect: Connect a crossconnect CAT5 or better cable from the IPSI adapter to the left port (Eth2) on the dual NIC.

For a connectivity guide, see *Quick Start for Hardware Installation: Avaya S8500 Media Server* (555-245-703).

Programming the IPSI circuit packs

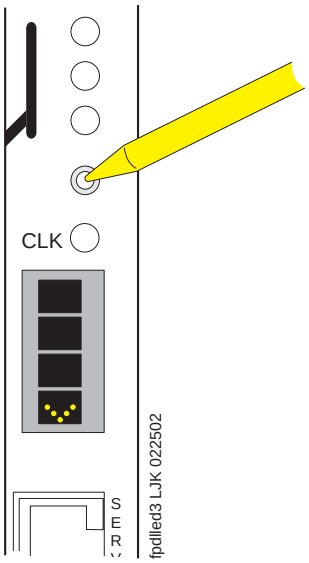
For the TN2312BP IPSI circuit packs to get IP addresses dynamically, you must first assign the switch ID (A through J) and the cabinet number (01 through 64) to each IPSI circuit pack. For G650 Media Gateways, a cabinet is defined as one or more media gateways connected by TDM cable, which is called a G650-rack-mount-stack.

Administering the location assignment

1 Fully insert the TN2312BP IPSI circuit pack. If necessary, reseat the circuit pack to begin the programming sequence.

NOTE:
You must do the following steps within 5 seconds after inserting the circuit pack.

2 Insert a pen, golf tee, or similar object (no graphite pencil) into the recessed push button switch.



NOTE:
If you pass up the letter or number that you want, you must either cycle through all the letters or numbers to get to the one you want or reinsert (reseat) the circuit pack and begin again.

Setting the switch ID

If you have only one system, the default switch ID is A. The second system would be B and so on. The switch ID is *not* the media gateway or carrier letter.

1 While the display is flashing, press the button until the switch ID (A through J) shows on the top character of the LED display. When the correct letter shows, stop. It will flash a few times (5 seconds) then stop. The next character down begins to flash.

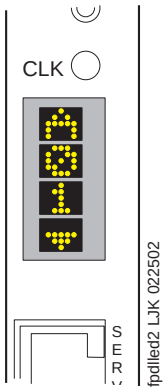
Setting the cabinet number

The number to program is the cabinet number *not* the port network number. If you have more than one IPSI in a cabinet, they all have the same cabinet number.

1 While the first digit of the number is flashing, press the button until the correct tens digit (0 through 6) shows on the display. When the correct digit shows, stop. It flashes a few times then stops (five seconds). The second digit begins flashing.

2 While the second digit is flashing, press the button until the correct units digit (0 through 9) shows on the display. When the correct digit shows, stop. The digit flashes a few times then stops (five seconds).

3 All segments of the display goes dark for one second, and then the Switch ID and media gateway stack number is displayed in the top three characters of the LED display. A "V" is shown in the fourth character (bottom) of the display. When the DHCP server assigns an address to the IPSI, the center of the "V" is filled in to form the bottom half of a diamond in the display.



For duplicated control network, repeat these steps for the second IPSI in the cabinet.

For the IPSI circuit packs to get static IP addresses, you must administer them directly through the Ethernet port connection on the IPSI faceplate (top port). See Figure 2, Connecting directly to the IPSI, on page 63.

Figure 2: Connecting directly to the IPSI

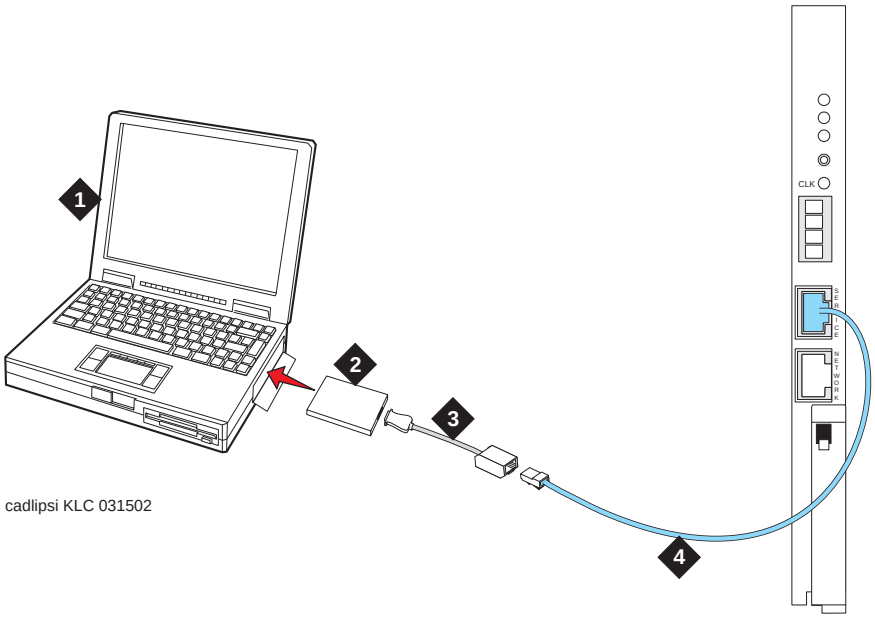


Figure notes

1	Services laptop	**3**	NIC adapter cable (if necessary)
2	PCMCIA Network Interface Card (NIC)	**4**	CAT5 crossover cable to IPSI

NOTE:
Make sure you have the password before proceeding.

1. Connect the services laptop computer to the top port on the IPSI circuit pack faceplate.
2. From the services laptop Start Menu, click **Start > Run** to open the Run dialog box.
3. Type **command** and press **Enter** to open a MS-DOS Command Line window.
4. Type **arp -d 192.11.13.6** and press **Enter** to clear the ARP cache in the laptop. This command responds with one of the following:
   - The command line prompt when the cache has been cleared.
   - The phrase: The specified entry was not found. This is returned when the specified IP address does not currently contain an entry in the ARP cache.
5. Type **telnet 192.11.13.6** and press **Enter** to open the Telnet window and connect to the IPSI

   Prompt = [IPSI]:

   NOTE:
   While connected to the IPSI, type **help** or **?** to obtain online help. Most commands have two or three letter abbreviations.

6. Type **ipsilogin** and press **Enter** (abbreviated command = **il)**.

   NOTE:
   The *craft* login used on the IPSI has a different password than the *craft* login used on the media servers.

7. Log in as **craft**.

   Prompt = [IPADMIN]:

Type show control interface and press Enter.

8. Type **show port 1** and press **Enter** to see the current settings.

9 Type **set control interface *ipaddr netmask*** and press **Enter**, where ***ipaddr*** is the customer-provided IP address and ***netmask*** is the customer provided subnet mask.

```
TN2312 IPSI IP Admin Utility
Copyright Avaya Inc, 2000, 2001, All Rights Reserved

[IPSI]: ipsilogin

Login: craft
Password:

[IPADMIN]: set control interface 135.9.70.77 255.255.255.0

WARNING!! The control network interface will change upon exiting IPADMIN


[IPADMIN]: show control interface

Control Network IP Address = 135.9.70.77
Control Network Subnetmask = 255.255.255.0
Control Network Default Gateway = None
IPSI is not configured for DHCP IP address administration

[IPADMIN]:
```

10 Press **Enter** to effect the changes.

11 Type **show control interface** and press **Enter**.
The IP address, subnet mask, and default gateway information will be displayed.
Verify that the proper information was entered.

12 If required, type **set control gateway *gateway*** and press **Enter**, where ***gateway*** is the customer-provided IP address for their gateway.

13 Press **Enter** to effect the changes.

14 If required, use the **set vlan priority**, **set vlan tag**, **set vlan id**, **set port negotiation** (1=disable), **set port duplex** (1 full), **set port speed** (1 100 MB), and **set diffserv** commands to enter VLAN and diffserv parameters for the IPSI. Use **Help** to obtain syntax guidelines for these commands.

15 Type **reset** and press **Enter**
Answer **Y** to the warning.

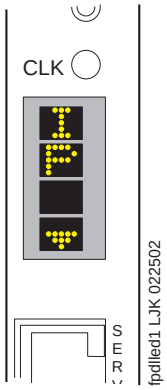
NOTE:
Resetting the IPSI terminates the administration session. If further administration is required, start a new telnet session to the IPSI.

16 Type **quit** to logoff the IPSI.

NOTE:
Control network settings (IP address, subnet mask, and gateway) become effective when you exit the IPADMIN session.

17 Check the LCD. Verify that it has an I P with a filled-in V showing at the bottom. (See Figure 3, LED display showing that the IPSI has a static IP address, on page 66)

Figure 3: LED display showing that the IPSI has a static IP address



18 Disconnect the laptop from the faceplate.

NOTE:
Always use the **arp -d 192.11.13.6** command (step 4) to clear the ARP cache on the laptop before connecting to another IPSI. If the cache is not cleared the laptop appears to hang and does not connect to the next IPSI.

19 Repeat for each IPSI circuit pack.

Verifying that IPSIs are translated

1 Type **list ipserver-interface** and press **Enter**.

2 Verify that all ISPI circuit packs are translated.

Verifying connectivity to media server

1 If not already open, open a browser and log in as **craft**.

2 Click **Launch Maintenance Web Interface**.

3 Under Diagnostics, click **Ping** and select **Other server(s)**, **All IPSIs**, **UPS(s)**, **Ethernet switches** to verify connectivity to these units.

4 Click **Execute Ping**.

5 Verify that all endpoints respond correctly.

Upgrading IPSI firmware version (if necessary)

You may need to upgrade the firmware on some or all the IPSIs. All IPSIs must be on the same firmware load.

1. Under IPSI Firmware Upgrades click **IPSI Version**.
2. Select **Query All** and click **View IPSI Version**.
3. Verify the firmware release for each TN2312BP IPSI. If an upgrade is required, follow the procedures in*Upgrading Software and Firmware—Avaya S8500 Media Server* (555-245-111), Upgrading IPSI Firmware.

Enabling control of IPSIs

NOTE:
Make sure the IPSIs have the same, current firmware.

NOTE:
This procedure enables the IPSI circuit packs and allows them to control the port networks.

1. Type **change system-parameters ipserver-interface** and press **Enter**.

```
change system-parameters ipserver-interface                    Page   1 of   1
                IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION

                IPSI Host Name Prefix:
      Primary Control Subnet Address: 172. 22.  0.  0
    Secondary Control Subnet Address:    .   .   .

OPTIONS

                    Switch Identifier: A
        IPSI Control of Port Networks: enabled
```

2. Make sure the **IPSI Control of Port Networks:** field is set to **enabled**.
3. Press **Enter** to effect the changes.

Verifying license status

1. Under Security, click **License File** and verify that the license mode is now normal.

Reusing a TN2312AP/BP circuit pack

On occasion a customer may want to reuse a TN2312AP or TN2312BP circuit pack that was previously programmed for DHCP or static addressing. You must erase the existing programming before reprogramming it. Failure to do this may result in serious network problems.

For information on erasing the programming, go to the *Maintenance Procedures for Avaya Communication Manager 2.1, Media Gateways and Servers* (03-300192).

4 Translating the IPSIs

These steps are done by issuing SAT commands on a terminal emulation program such as Avaya Native Configuration Manager, Avaya Terminal Emulation, or HyperTerminal. You also can use Avaya Site Administration, part of the Avaya Integrated Management suite, which you can purchase from Avaya.

> **NOTE:**
> You must use Release 1.11 or a later version of Avaya Site Administration, to administer new features in Release 2.1 of Avaya Communication Manager.

Perform these tasks to customize the media server:

- Starting terminal emulation on page 69
- Inputing translations on page 70
- Resetting the media server on page 70
- Adding media gateways on page 70
- Administering the IPSIs on page 71

Starting terminal emulation

> **NOTE:**
> Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are supported terminal emulation applications.

1. On the services laptop, open a VT-100 terminal emulation session.
2. Administer the terminal emulation port settings:
   - 9600 baud
   - No parity
   - 8 data bits
   - 1 stop bit
   - No flow control
   - 5023 for the port
3. Log into the media server as **craft**.

Inputing translations

Contact the installation personnel responsible for translation input to download the translations.

1 Type **save translations** and press **Enter** to save the translations to the hard drive.

If the translations are not ready, you may continue with the process, entering minimal translations to verify connectivity to the port networks.

Resetting the media server

NOTE:
Do not reset the media server if no translations were input or if they were not entered in bulk.

1 Type **reset system 4** and press **Enter** to have the software read the copied translations.

Adding media gateways

NOTE:
Do this procedure only if the translations were *not* input earlier.

NOTE:
A cabinet is defined as up to 5 G650 Media Gateways mounted in a rack and TDM-connected or 1 MCC1 Media Gateway.

1 Type **add cabinet *number*** (1 through 64) and press **Enter** for each stack of G650 Media Gateways or MCC1 Media Gateway controlled by one TN2312BP IPSI circuit pack.

2 Fill in the location and carrier type for media gateways 2(B), 3(C), 4(D), and 5(E).

```
add cabinet 1                                                Page   1 of   1
                                    CABINET
 CABINET DESCRIPTION
                  Cabinet: 9
            Cabinet Layout: G650-rack-mount-stack
              Cabinet Type: expansion-portnetwork


                 Location: 1

 Rack:               Room:              Floor:             Building:

 CARRIER DESCRIPTION
   Carrier       Carrier Type        Number

      E        not-used             PN  09
      D        not-used             PN  09
      C        not-used             PN  09
      B        G650-port            PN  09
      A        G650-port            PN  09
```

Administering the IPSIs

NOTE:
This procedure enables the IPSI circuit packs and allows them to control the port networks.

1 Type **change system-parameters ipserver-interface** and press **Enter**.

```
change system-parameters ipserver-interface                    Page   1 of   1
                IP SERVER INTERFACE (IPSI) SYSTEM PARAMETERS

SERVER INFORMATION

                IPSI Host Name Prefix:
      Primary Control Subnet Address: 172. 22.  0.  0*
    Secondary Control Subnet Address: 192. 11 . 13 .4*

OPTIONS

                    Switch Identifier: A
        IPSI Control of Port Networks: enabled




              NOTE: * indicates data changed on the server
```

2 Verify that the Primary Control Subnet Address is correct.

The subnet address must match the most significant 3 octets (the first 3 groups of digits in the subnet address) of the Server IP address.

An Asterisk (*****) to the right of the **Subnet Address** field means that although a subnet address is displayed, it is not the correct one; Avaya Communication Manager does not have the subnet information. After verifying the displayed information, submit this form with or without changes to update software with the correct subnet information.

CAUTION:
If the information displayed in the **Subnet Address** field is not correct, it must be changed on the media server. Use the Maintenance Web Interface; under Server Configuration and Upgrades, click **Configure Server** to change the media server configuration. Then return here to perform this step.

3 Set the **Switch Identifier:** field to the switch ID letter (A thru J; A is the default setting).

4 Set the **IPSI Control of Port Networks:** field to **enabled**.

5 Press **Enter** to effect the change.

Adding IPSI information

1. Type **add ipserver-interface *PNnumber*** and press **Enter** to add the IPSI circuit pack information.
2. For static addressing, in the **Host:** field, type in the IP address for the IPSI in the port network listed in the **Location:** field.

```
add ipserver-interface 8
          IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 8

IP Control? y                                          Socket Encryption? y

                                                                Enable QoS? y

 Primary IPSI                                          QoS Parameters
 ------------                                          --------------
  Location:  1A01                                        Call Control 802.1p: 6
      Host: 172.22.22.174                              Call Control DiffServ: 46
   DHCP ID: ipsi-A01a


 Secondary IPSI
 --------------
  Location:  1B01
      Host: 172.22.22.175
   DHCP ID: ipsi-A01b
```

3. Set the **IP Control?** field to **y**.
4. Verify that all the other fields are populated.
5. Press **Enter** to effect the changes.
6. Repeat steps 1 through 5 for each port network.

Setting alarm activation level

1. Type **change system-parameters maintenance** and press **Enter**.

```
change system-parameters maintenance                                  Page 1 of 3

                    MAINTENANCE-RELATED SYSTEM PARAMETERS

OPERATIONS SUPPORT PARAMETERS
     CPE Alarm Activation Level: none

SCHEDULED MAINTENANCE
                            Start Time: 22 : 00
                             Stop Time: 06 : 00
                      Save Translation: daily
 Update LSPs When Saving Translations: y
             Command Time-out (hours): 2
          Control Channel Interchange: no
       System Clocks/IPSI Interchange: no
```

2 In the **CPE Alarm Activation Level** field, select **none** (default), **warning**, **minor**, or **major**, depending on the level the customer wants and press **Enter** to effect the changes.

3 Repeat for each IPSI.

Installing the translation file

1 Type **save translations** and press **Enter** to save the translations to the hard drive.

5 Completing the installation administration

This section covers the following tasks:

- Verifying translations on page 75
- Setting daylight savings time rules on page 76
- Setting locations (if necessary) on page 77
- Verifying date and time on page 77
- Resolving alarms on page 78
- Backing up files to the compact flash media on page 78
- Telneting to media server on page 80
- Enabling alarms on page 80
- Registering the system on page 81

Verifying translations

1. Type **list configuration all** and press **Enter** to view all the administered circuit packs in the system.
2. Type **list ipsi** and press **Enter** to verify the location of the IPSI circuit packs.
3. Check the administration status on the following items:
   - **list station**
   - **list trunk-group**
   - **list hunt-group**

   NOTE:
   Even though you set the date, time, and time zone through the Web interface on the media server, you also must set the daylight savings time rules and locations and verify the date and time through SAT commands.

Setting daylight savings time rules

You can set up to 15 customized daylight savings time rules. If you have media gateways in several different time zones, you can set up rules for them on a per-location basis. A daylight savings time rule specifies the exact time when you want to transition to and from daylight savings time. It also specifies the increment at which to transition.

NOTE:
The default daylight savings rule is **0**, meaning no daylight savings transition.

1 Type **change daylight-savings-rules** and press **Enter**.

```
change daylight-savings-rules                                    Page   1 of   2
                      DAYLIGHT SAVINGS RULES

 Rule          Change Day                 Month  Date   Time    Increment

  0: No Daylight Savings

  1: Start: first Sunday     on or after April     1   at 02:00   01:00
     Stop: first Sunday      on or after October   25  at 02:00
  2: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  3: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  4: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  5: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  6: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
  7: Start: first            on or after               at   :       :
     Stop: first             on or after               at   :
```

2 In the **Change Day**, **Month**, **Date**, **Time**, and **Increment** fields, type the appropriate Start and Stop information for each rule. For example, **1:00** in the **Increment** field means to move the clock forward or back by one hour at the transition point.

NOTE:
You can change any rule except rule 0 (zero). You cannot delete a daylight savings rule if it is in use on either the ***Locations*** or ***Date and Time*** screens.

3 When done, press **Enter** to effect the changes.

Setting locations (if necessary)

After you set the daylight savings rules, you must set the locations for all media gateways (cabinets). It is possible to have media gateways in different time zones.

1 Type **change locations** and press **Enter**.

```
change locations                                          Page   1 of   5
                                  LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Number  Name              Timezone  Daylight-Savings        Number Plan
                            Offset   Rule                    Area Code
   1     Main              + 00:00   0
   2     CA                - 02:00   0
   3                           :
   4                           :
   5                           :
   6                           :
   7                           :
   8                           :
   9                           :
  10                           :
  11                           :
```

2 In the **ARS Prefix 1 Required for 10-Digit NANP Calls?** field, type **y**.

3 Type the information in the various fields for each media gateway.

> **NOTE:**
> In the **Name** field for location 1, call the media gateway (cabinet) Main.

4 Press **Enter** to effect the changes.

Verifying date and time

1 Type **display time** and press **Enter**.

```
display time                                                Page   1 of   1
                              DATE AND TIME

        DATE

            Day of the Week: Friday         Month: November
           Day of the Month: 8               Year: 2002

        TIME

            Hour: 14  Minute: 19    Second: 36   Type: Standard

                       Daylight Savings Rule: 0

  WARNING: Changing the date or time may impact BCMS, CDR, SCHEDULED
```

2 Verify that the date and time are correct.

3. Verify that the correct rule (number) is displayed in the **Daylight Savings Rule** field.
4. If correct, press **Cancel**.
5. If not, go to the Maintenance Web Interface.
6. Under Server, click **Set Server Time/Timezone**.
7. Verify that the date and time are correct. If not, set it here.
8. Repeat steps 1 through 3.

Resolving alarms

1. Under Alarms click **Current Alarms**.
2. Select the server alarms to be cleared and click **Clear**.
3. Resolve any major alarms using SAT commands and a terminal emulation application, such as Native Configuration Manager or MS HyperTerminal.

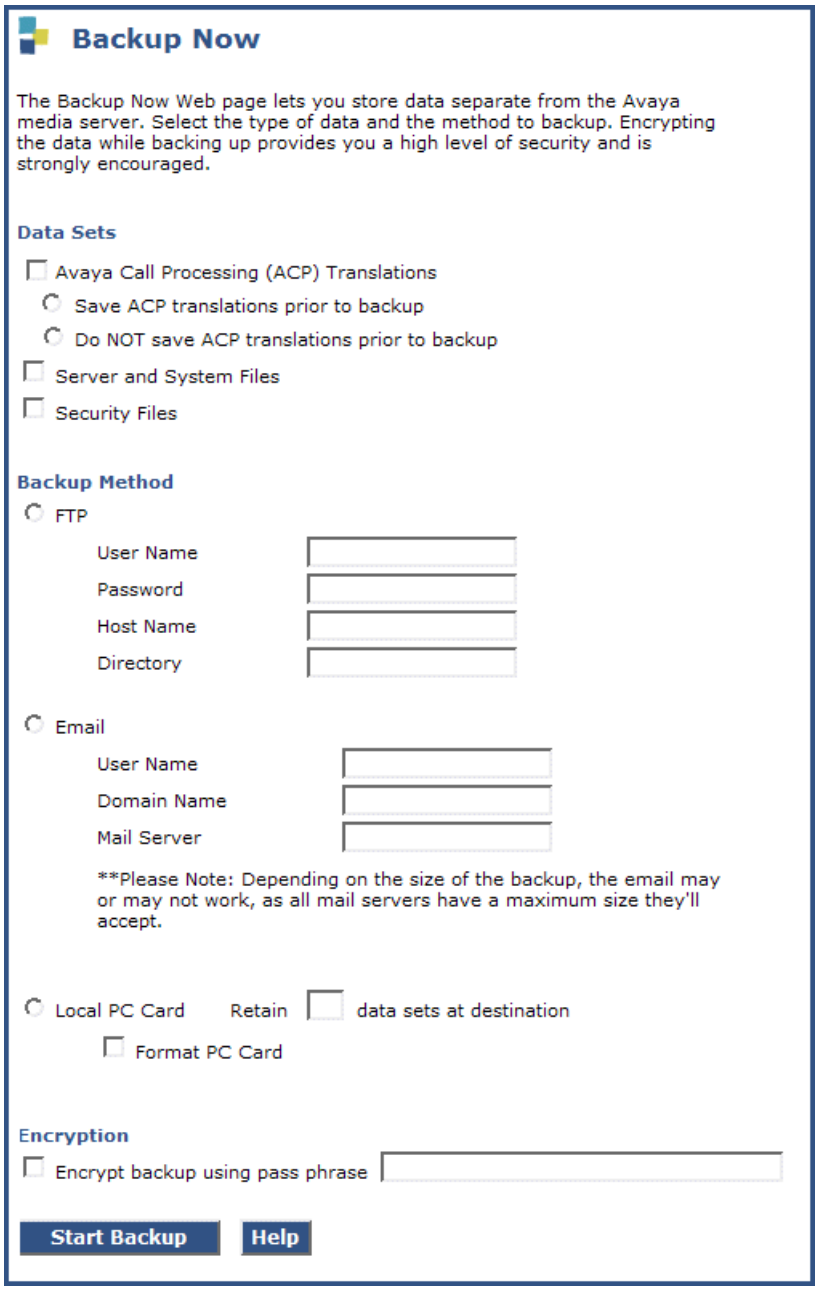
Backing up files to the compact flash media

1. Connect the compact flash drive to one of the USB ports on the front of the media server.
2. Insert a 128-Mb compact flash media into the top right slot of the drive.

NOTE:
The industrial grade compact flash media provides improved data integrity and reliability, enhanced durability, and extreme endurance. For these reasons Avaya recommends the use of an industrial grade compact flash. To read more about the industrial grade compact flash, see the *Hardware Guide for Avaya Communication Manager* (555-245-207).

NOTE:
You must format the compact flash media before writing to it.

3 Under Data Backup/Restore click **Backup Now**.


Backup Now
The Backup Now Web page lets you store data separate from the Avaya media server. Select the type of data and the method to backup. Encrypting the data while backing up provides you a high level of security and is strongly encouraged.
Data Sets
Avaya Call Processing (ACP) Translations
Save ACP translations prior to backup
Do NOT save ACP translations prior to backup
Server and System Files
Security Files
Backup Method
FTP
User Name
Password
Host Name
Directory
Email
User Name
Domain Name
Mail Server
**Please Note: Depending on the size of the backup, the email may or may not work, as all mail servers have a maximum size they'll accept.
Local PC Card
Retain
data sets at destination
Format PC Card
Encryption
Encrypt backup using pass phrase
Start Backup
Help

4 Select all applicable data sets.

5 Select either Local PC Card and Format PC Card, or Format PC Card (the second such selection further down the screen).

Use Local PC Card and Format PC Card to format the PC card and back up the data onto it.

Use Format PC Card to format new cards or to overwrite an existing card.

NOTE:
Customer's may want to back up using another method.

6 Click **Start Backup.** You are notified when the format is completed (approximately 10 seconds).

NOTE:
Clicking on **Start Backup** without media in the compact flash drive results in an error. To continue with the backup, unplug the drive, insert the formatted media into the right top slot, and plug the drive back into the USB port.

7 Click **Backup Status** to view the status of the backup.

Telneting to media server

Enabling alarms uses Linux commands through Telnet.

1 Click **Start** > **Run** to open the ***Run*** dialog box

2 Type **telnet 192.11.13.6** and press **Enter**.

3 Log in as **craft** or **dadmin** (if business partner).

Enabling alarms

To INADS via modem

1 Type **almenable -d b** and press **Enter.**

2 Type **almenable** and press **Enter** to verify that the alarms are enabled.

To INADS via SNMP

NOTE:
Do these steps only if a Secure Service Gateway (SSG) is being installed.

1 Type **almsnmpconf -d *ipaddress* -c *communityname*** and press **Enter**, where *ipaddress* is the trap receiver address for the SSG device and *communityname* is the community string name required by the SSG device.

2 Type **almsnmpconf** and press **Enter**.

Verify that the correct information was entered.

3 At the prompt, type **almenable -s y** and press **Enter**.

4 Type **almenable** and press **Enter**.

Verify that the SNMP alarm origination is enabled. If used, verify that alarm origination via modem is still enabled.

5 Log off.

Registering the system

Follow the existing process and procedures to register the Avaya S8500 Media Server.

Let customers know what the default LAN security settings are; they may want to change them after installation. Make sure they are aware that if the following items are not enabled, they will not have remote access to the media server:

- telnet—no Telnet access
- https—no Maintenance Web Interface access
- def-sat—no SAT command access

6 Installing the media gateways

In a new installation, the Avaya S8500 Media Server works with only the Avaya G650 Media Gateway.

In a migration the media server works with Avaya MCC1, SCC1, G600, or CMC1 Media Gateways.

In addition, the media servers work with Avaya G350 and G700 Media Gateways, but only if the G650 Media Gateway has a TN799DP C-LAN circuit pack installed. These gateways are treated as endpoints off the TN799DP.

Media gateways typically are installed in the same equipment room as the media server rack hardware (control network); however, they can be installed in another location, including another state or country.

For information on installing media gateways, see

- *Installing the Avaya G650 Media Gateway* (03-300144)
- *Quick Start for Hardware Installation: Avaya G350 Media Gateway* (03-300148)
- *Installation of the Avaya G350 Media Gateway* (555-245-104)
- *Quick Start for Hardware Installation: Avaya S8300 Media Server and Avaya G700 Media Gateway* (555-233-150)
- *Installation and Upgrades for the Avaya G700 Media Gateway and Avaya S8300 Media Server* (555-234-100)

7 Testing the media server installation

This chapter provides tests for the control network, including

- reviewing the status of the configuration.
- testing the IPSI circuit packs.

In addition, it provides information on the LED status indicators for the media servers, Avaya Ethernet switch(es), uninterruptible power supplies (UPSs), and different circuit packs. See LED indicators on page 87.

NOTE:
Circuit pack positions are usually given by cabinet, and slot. They may also be given by port. The term cabinet refers to five G650 Media Gateway TDM-cabled together in a rack, making up one port network. A port network is defined as a group of media gateways connected together with one TDM bus.

Perform these tasks to test the configuration:

CAUTION:
To prevent unnecessary trouble tickets, do not enable the alarms (Alarm Origination feature) until all installation and administration procedures are completed.

- Testing the TN2312BP IPSI circuit pack on page 85
- Testing the license file on page 86

NOTE:
Do these steps using a SAT session

Testing the TN2312BP IPSI circuit pack

1. Type **test ipserver-interface *UUC*** and press **Enter** to test all clock and packet interface components within the IPSI circuit pack.
2. Verify the screen displays ***Test Results*** screen similar to Figure 4, Sample IPSI 01A test results screen—page 1, on page 86.

Figure 4: Sample IPSI 01A test results screen—page 1

```
test ipserver-interface 1a                                          Page   1

                                TEST RESULTS

Port        Maintenance Name  Alt. Name Test No. Result           Error Code

01A         TONE-BD                     46       PASS
01A         TONE-BD                     52       PASS

               press CANCEL to quit --  press NEXT PAGE to continue
```

Testing the license file

CAUTION:
Wait at least 30 minutes after you install the license before you do the test.

1. Type **test license [short | long]** and press **Enter**.
2. Verify the screen displays a ***Test Results*** screen similar to Figure 5, Sample test results screen for test license, on page 86.

Figure 5: Sample test results screen for test license

```
test license

                                TEST RESULTS

Port        Maintenance Name  Alt. Name Test No. Result           Error Code

            LIC-ERR                     1484     PASS
```

LED indicators

See the *Maintenance Alarms for Avaya Communication Manager 2.1, Media Gateways and Servers* (03-300190) for detailed alarm and LED descriptions. If a maintenance object begins to fail some periodic tests, the media server generates an alarm. The media server identifies three levels of alarms:

- Major Alarms—Failures that cause critical degradation of service and require immediate attention.
- Minor Alarms—Failures that cause some degradation of service, but do not cause a critical portion of the configuration to be inoperable. This condition requires action, but its consequences are not immediate. Problems might be impaired service to a few trunks or stations or interfering with one feature across the entire configuration.
- Warning Alarms—Failures that cause no significant degradation of service or failures in equipment external to the configuration. Warning alarms are not reported to the attendant console or INADS.

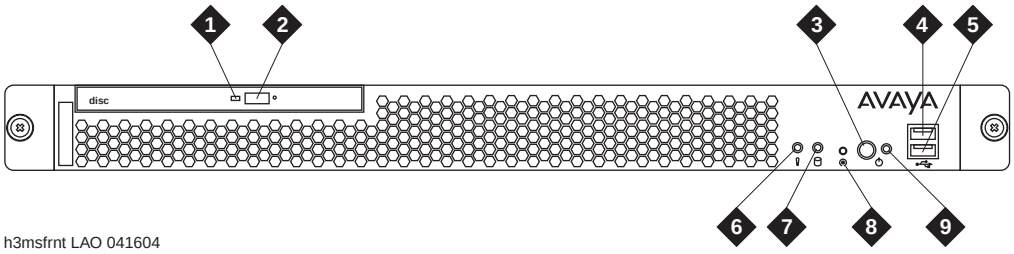
Alarms are communicated to users and technicians by entries in the alarm and system logs and the lighting of LEDs located on the media server.

More detailed information is available here for:

- Avaya S8500 Media Server LEDs on page 88
- Avaya Ethernet switch LEDs on page 89
- Uninterruptible power supply LEDs on page 90
- IPSI LEDs on page 90

Avaya S8500 Media Server LEDs

Figure 6: Front of the Avaya S8500 Media Server



Number	Description
1: CD-ROM drive activity	When lit, the CD-ROM drive is in use.
2: CD eject button	Press to release a CD from the CD-ROM drive.
3: Power-control button	Press to turn the server on or off manually.
4: USB connector 1	This USB port configures automatically and uses a serial interface standard for telephony and multimedia devices.
5: USB connector 2	This USB port configures automatically and uses a serial interface standard for telephony and multimedia devices.
6: System-error LED (AMBER)	This lights when a system error occurs.
7: Hard disk drive activity	When flashing, it indicates that the associated hard disk drive is in use.
8: Reset button	Press to reset the server and run the power-on self-test (POST).
9: Power-on (GREEN)	When lit, it indicates that the server is turned on. When flashing, the processor is coming on.

The Avaya S8500 Media Server has five LEDs on the front and four LEDs in the back. The following is a brief description of the function of each LED:

- CD drive activity (GREEN): When lit, the CD-ROM drive is in use.
- Diskette drive activity (GREEN): When lit, the diskette drive is in use.
- System error (AMBER): Lights when a system error occurs.
- Hard disk drive activity (GREEN): When lit, the disk drive is in use.
- Power-on (GREEN): When lit, the server is turned on.
- Ethernet 1 activity (GREEN): Blinks when there is an active 10/100/1000BASE-T connection for Ethernet port 1.
- Ethernet 1 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The green LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.

- Ethernet 2 activity (GREEN): Blink when there is an active 10/100/1000BASE-T connection for Ethernet port 2.
- Ethernet 2 link (GREEN): Lights when the speed of the Ethernet LAN is 1000BASE-T. The green LED will be off when the speed of the Ethernet LAN is 10/100BASE-T.

A power LED on the RSA lights when one or both of the following conditions are met:

- The RSA is receiving power from the external power-supply adapter.
- The RSA is receiving power from the Avaya S8500 Media Server in which it is installed.

Avaya Ethernet switch LEDs

The Avaya Ethernet Switch P333T has the LEDs shown in Figure 7, LEDs on Avaya P333T Ethernet switch, on page 89:

Figure 7: LEDs on Avaya P333T Ethernet switch

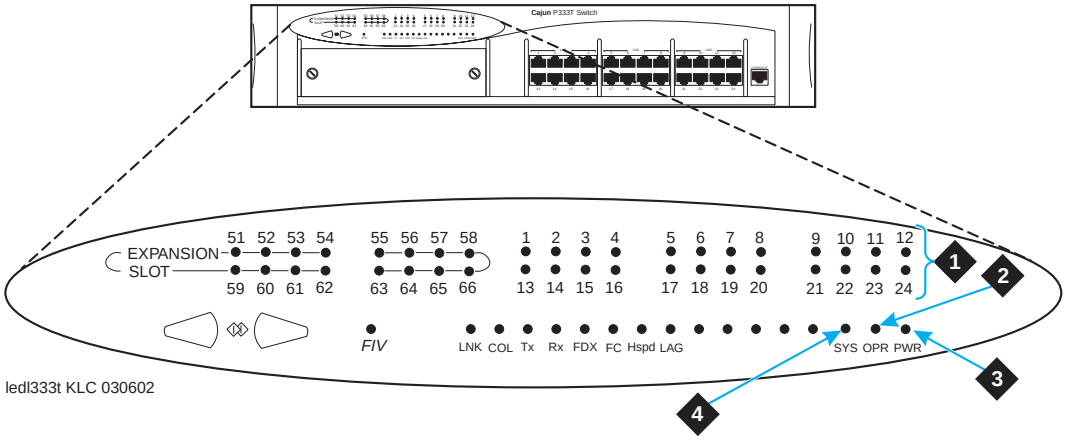


Figure notes

1	Ports in use	**3**	Power
2	CPU boot status	**4**	Lights if this module is the Avaya P33x stack master agent

For descriptions of the other LEDs, see the quick start guide and user guide that comes with the model of Avaya Ethernet switch you have.

Uninterruptible power supply LEDs

The Powerware uninterruptible power supply (UPS) front panel has the LEDs shown in Figure 8, LEDs on Powerware 9125 UPS, on page 90:

Figure 8: LEDs on Powerware 9125 UPS

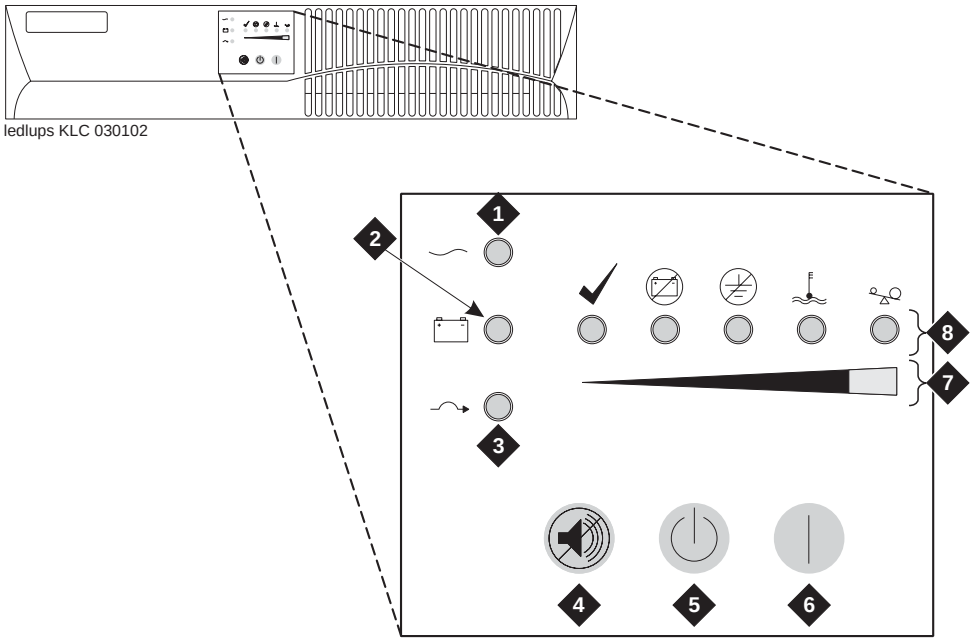


Figure notes

1	Normal mode indicator	**5**	Off button
2	Battery mode indicator	**6**	On button
3	Bypass mode indicator	**7**	Bar graph indicators
4	Test/Alarm reset button	**8**	Alarm indicators

After plugging in the UPS, all the LEDs flash briefly. After a self test, the Normal mode LED flashes, indicating that the UPS is in Standby mode.

For more information on the LEDs, see the UPS user's guide that comes with the Powerware UPS.

IPSI LEDs

The TN2312BP Internet Protocol Server Interface (IPSI) circuit pack LEDs are shown in Figure 9, TN2312BP circuit pack faceplate, on page 91). It also has a programmable LED display to indicate whether its IP address is dynamic (shows media gateway location) or static (shows I P). See Figure 10, LED display on the IPSI circuit pack—static address, on page 92.

Figure 9: TN2312BP circuit pack faceplate

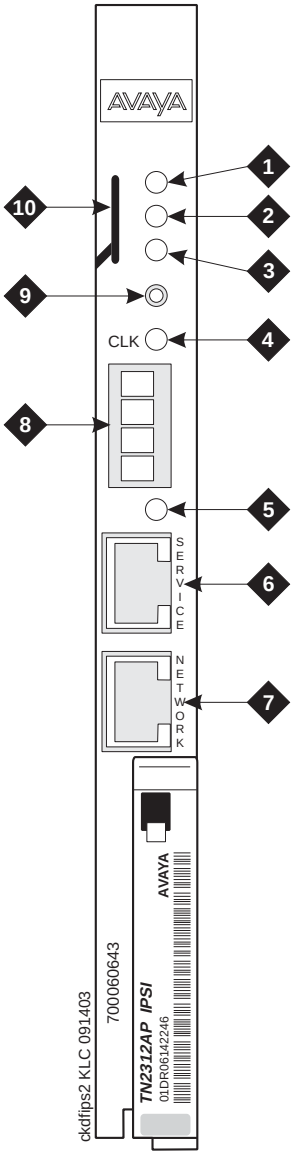


Figure notes

1	Red LED	**6**	Services RJ45 connector
2	Green LED	**7**	Network Control RJ45 connector
3	Amber LED	**8**	4-character LED display
4	Yellow LED (Tone Clock status)	**9**	Pushbutton switch
5	Emergency Transfer LED	**10**	Slot for maintenance cable

Figure 10: LED display on the IPSI circuit pack—static address

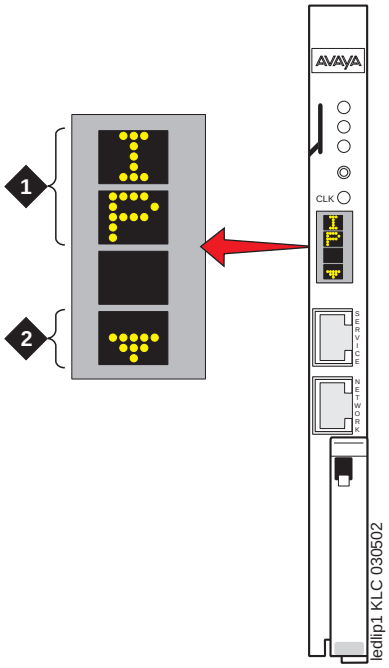


Figure notes

1	IPSI has a static IP address	**2**	IPSI has connectivity and an IP address

The display also indicates connectivity (see Figure 11, LED display indicating connectivity status—DHCP address, on page 93).

Figure 11: LED display indicating connectivity status—DHCP address

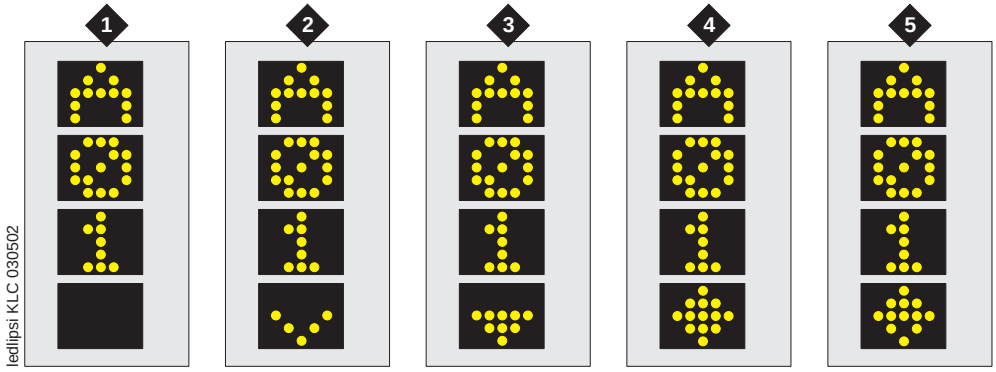


Figure notes

Connectivity status	1	2	3	4	5
IPSI is connected to media server	no	yes	yes	yes	yes
IPSI has an IP address	no	no	yes	yes	no
Laptop computer is connected to IPSI services port	no	no	no	yes	yes

A Accessing the media server

To administer the media server, you must be able to access it. Personal computers and services laptop computers equipped with a network interface card (NIC), a terminal emulation program, and a Web browser are the supported access points for accessing the media server for initial configuration, aftermarket additions, and continuing maintenance.

You can access the media server either directly or remotely over the customer's network or over a modem. Connecting directly and remotely over the customer's network are the preferred methods. Remote access over a modem is for Avaya maintenance access only.

This section covers the following sections:

- Connecting to the media server directly on page 95
- Connecting to the media server remotely over the network on page 97
- Connecting to the media server remotely over a modem on page 97
- Logins on page 99
- Network configuration on page 100

Connecting to the media server directly

You access the media server directly by plugging a laptop computer into the services port (port 2 [Eth1]) on the media server. See Figure 12, Services laptop computer connected directly to the S8500 Media Server, on page 96. The computer used for accessing the media server must have the following minimum specifications:

- Windows 2000/XP operating system
- 32-MB RAM
- 40-MB available disk space
- RS-232 port connector
- Network interface card (NIC) with a 10/100 BaseT Ethernet interface
- 10/100 BaseT Ethernet, category 5 (or better), crossconnect cable with an RJ45 connector on each end (MDI to MDI-X)
- CD-ROM drive

Plug one end of the CAT5 cable into the services access port, which defaults to port 2 (Eth1), on the back of the media server and the other end into the NIC on your computer. (You may need a NIC adapter.)

You also must configure your network connection. For specific information, see Network configuration on page 100.

The network connection for the computer is

- IP address: 192.11.13.5
- Subnet mask: 255.255.255.252

Figure 12: Services laptop computer connected directly to the S8500 Media Server

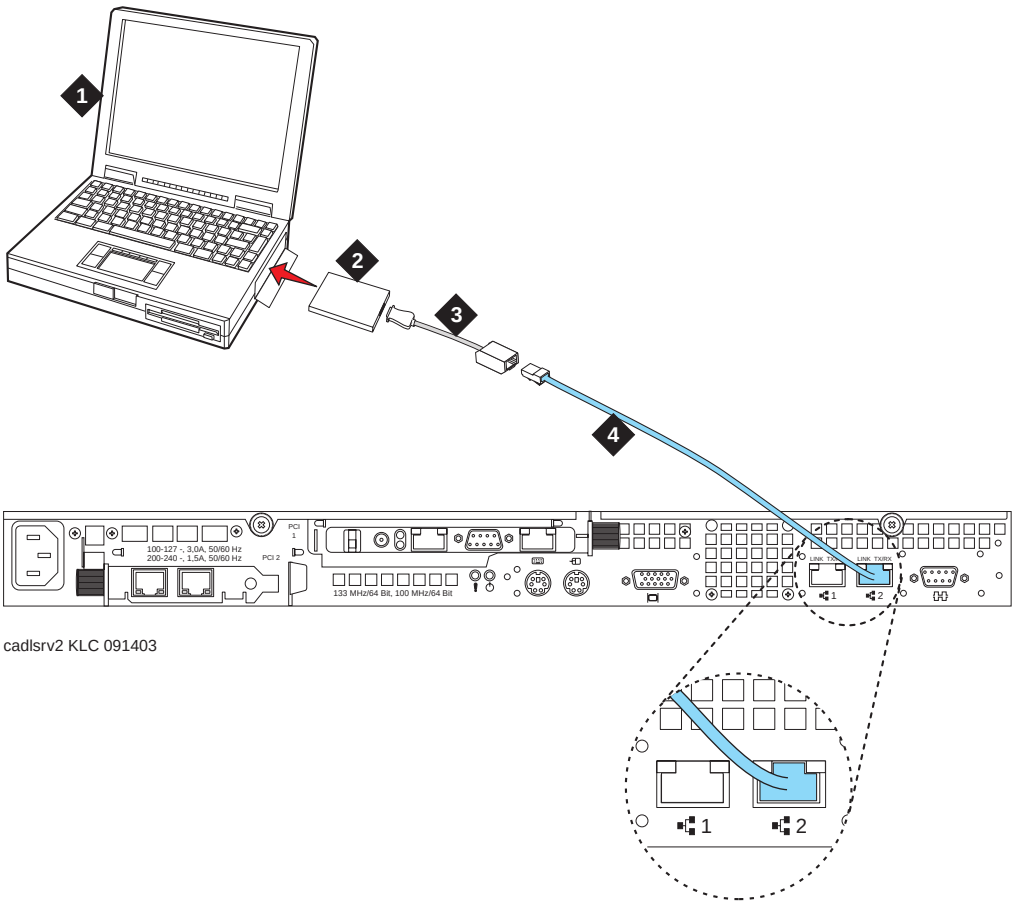


Figure notes

1	Services laptop	**3**	NIC adapter cable (if necessary)
2	Network interface card (NIC)	**4**	Black CAT5 crossconnect cable

Once connected, you can administer the media server using these interfaces:

- Maintenance Web Interface for server-specific administration.
- A command line interface in a Telnet or terminal emulation application for Linux and SAT commands (usable on the active media server only).

See Accessing the Maintenance Web Interface on page 98 for more details.

Connecting to the media server remotely over the network

You can access the media server from any computer connected through the LAN. However, make sure the LAN security settings allow remote access.

To access the media server, open a Web browser or a terminal emulation application. In the address field, type in the IP address or DNS host name assigned to the media server you want to access.

Connecting to the media server remotely over a modem

This section covers the following tasks:

- Setting up a dial-up connection on page 97
- Dialing up to the media server on page 98
- Accessing the Maintenance Web Interface on page 98
- Using the command line interface on page 98

NOTE:
Remote access over a modem is for Avaya services support access only and not for routine administration. Because the media server uses the same line to report alarms, it cannot report new alarms while the line is in use.

You can access the media server through an analog modem. The remote connection requires a data speed of at least 33.5 kilobits per second.

You also can access the Remote Supervisor Adapter (RSA) installed in the media server remotely using the attached serial modem. The serial modem and the USB modem both share the same telephone line. When the media server is healthy, the incoming call over the shared telephone line is answered by the USB modem. In the event the media server is down, the serial modem on the RSA answers the call. For more information on accessing the RSA, see Connecting and logging into the adapter on page 52.

Setting up a dial-up connection

To use a computer modem, you first must set it up through your dial-up connection.

1. Launch the dial-up connection program, which varies depending on your operating system. Generally, you can access them through My Computer or Control Panel folders. See your computer's help system for specific information.
2. Double-click **Make New Connection** to open the New Connection wizard.
3. Within the wizard, and depending on your operating system, you may be asked to:
   - Assign a name to the connection.
   - Select dial-up to the network for the network connection type.
   - Select the modem you will be using for the dial-up connection.

- Type in the appropriate telephone number to access the active server. See the filled-out job aid titled *Electronic Preinstallation Worksheet* for the customer-supplied telephone number(s).
- Under Advanced, select **PPP** and log on manually. You may have to type in a user name and password, depending on whether or not the media server you are dialing into has a non-null CHAP secret key. Use **craft** (ignore the password field).

Dialing up to the media server

To dial up, click the connection name or icon, if created. Once you are connected:

1. When prompted, enter your remote access login name and password.
2. When the `Start PPP now!` message appears, click **Done**. When you see the Connection Complete dialog box, your computer is connected to the media server.
3. To open a Telnet session, click **Start** > **Run** to open the **Run** dialog box.
4. In the Run dialog box, type **telnet *IPaddress*** and click **OK**, where ***IPaddress*** is the address of the actual active media server.

Accessing the Maintenance Web Interface

You can access the Maintenance Web Interface either by connecting directly to the services port (port 2 [Eth1]) on the media server (see Figure 12, Services laptop computer connected directly to the S8500 Media Server, on page 96) or connecting over the customer's network. The only browser supported is MS Internet Explorer 5.5 or 6.0.

When connected *directly* to the media server, you must disable all proxy servers. See Browser settings on page 101 for instructions.

1. Open the MS Internet Explorer Web browser.
   - If a direct connection, in the **Address** field, type **192.11.13.6**.
   - If a remote connection, in the **Address** field, type in the IP address or DNS host name of the media server.
2. When prompted, log in.

Using the command line interface

Telnet: To use a command line interface in a Telnet window:

1. Click **Start** > **Run** to open the **Run** dialog box.
   - If a direct connection, type **telnet 192.11.13.6** and click **OK**.
   - If a remote connection, type in the IP address of the media server.
2. When prompted log in.

Terminal Emulation: To use a command line interface in a terminal emulation window open your terminal emulation application. The terminal emulation program port settings must be configured as follows:

- 9600 baud
- No parity
- 8 data bits
- 1 stop bit
- No flow control

> **NOTE:**
> Avaya Native Configuration Manager, Avaya Terminal Emulation, and HyperTerminal are the only terminal emulation programs supported.

Establish a network connection to the media server using either the IP address or the DNS host name. Use port **5023** for this connection. When prompted, log in.

Logins

Initial configuration and upgrades by an Avaya field tech or business partner requires a services login, such as craft or dadmin, assigned to the customer's system.

After installing the Avaya authentication file, Avaya Communication Manager has a password for the craft login that is unique to the customer's system and available when connected directly to the media server. To bypass the ASG challenge and response, use this password the next time you log in as **craft**. Every other means of craft access still require an ASG challenge and response. The revised password is recorded by RFA and is obtained from ASG Conversant at 1-800-248-1234 or 1-720-444-5557.

Customer's can set up their own logins for accessing Avaya's media servers. See the *Avaya Communication Manager Little Instruction Book for Basic Administration* (555-233-756) for specific information. You must have superuser permission to create or change logins and passwords.

> **NOTE:**
> When assigning login IDs, do not start them with a number.

Network configuration

NOTE:
Write down the original settings in case you need to change them back.

A new network connection must be configured as follows:

NOTE:
These instructions are for Windows 2000/XP only.

1. On your computer desktop, right-click **My Network Places** and left-click **Properties** to display the ***Network Connections*** window.

   Windows 2000/XP should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection may appear.

2. Right-click on the correct **Local Area Connection** and left-click **Properties** to display the ***Local Area Connection Properties*** dialog box.
3. Select **Internet Protocol (TCP/IP)**.
4. Click **Properties** to display the ***Internet Protocol (TCP/IP) Properties*** dialog box.
5. On the General tab, select **Use the following IP address**. Enter the following:
   - IP address: **192.11.13.5**
   - Subnet mask: **255.255.255.252**

   Make a note of any IP addresses or other entries that you have to clear. You may need to restore them later to connect to another network.
6. Select **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
7. Click **Advanced** at the bottom of the dialog box to display the Advanced TCP/IP Settings dialog box.
8. Click the **DNS** tab. Make sure no DNS server is administered (the address field should be blank).
9. Click **OK**, **OK**, and **Close** to close all the windows.

Browser settings

Connecting directly to the media server

NOTE:
Instructions are for Internet Explorer 6.0 only.

1. Click **Tools** > **Internet Options**.
2. Select the **Connection** tab.
3. In the LAN Settings box (lower righthand), click Advanced
4. In the Exceptions box after the last entry, type **;192.11.13.6**
5. Click **OK**, then **OK**, then **OK** again to close all the dialog boxes.

Connecting remotely through the network

When connected through a proxy server, a connection session to a media server tends to time out. To avoid having the media server time out during a session, add the media servers' host names or IP addresses to the list of host names and IP addresses.

NOTE:
Instructions are for Internet Explorer 6.0 only.

1. Click **Tools** > **Internet Options**.
2. Select the **Connection** tab.
3. Click on **LAN settings**, then **Advanced**.
4. In the `Do not use proxy server for addresses beginning with`: field, type in the IP address for each media server you intend to access remotely. If the IP addresses have the first or first and second octets the same, you can shorten it to xxx.xxx.* (example, 135.9.*).
5. Click **OK**, then **OK**, then **OK** to close all the dialog boxes.

B Troubleshooting an installation

This section provides some simple strategies for troubleshooting an installation of a media server. It focuses on possible problems when

- Installing the media server hardware on page 103
- Configuring the media server hardware on page 104
- Installing the license and Avaya authentication files on page 105

Installing the media server hardware

The media server hardware includes the

- Media server(s)
- Ethernet switch
- Uninterruptible power supply (UPS)
- TN2312BP IP Server Interface circuit pack

Problem	Solution
No power to the UPS	- Make sure the UPS is plugged into the outlet. - Make sure the outlet has power. - See the user's guide that comes with UPS for other solutions.
No power to the Ethernet switch	- Make sure the Ethernet switch is plugged into the UPS or outlet. - Make sure the UPS or outlet has power. - See the user's guide that comes with the Ethernet switch for other solutions.
No power to the media server	- Make sure the media server is plugged into the UPS. - Make sure the UPS has power. - Push the power button on the front of the media server.
IPSI LEDs flash	- Make sure it is in the correct slot: (slot 1 for G650 Media Gateway, slot 2 for G600 Media Gateway, Tone-Clock slot for all others). - Ping IPSI from server. - Ping server from IPSI (it is connected to the top Services port on the IPSI).

Configuring the media server hardware

Problem	Solution
Cannot log into UPS subagent	- Make sure the SNMP Subagent is installed in the UPS. - Make sure you are connected to the correct Ethernet port. - Make sure you have the correct login ID and password. See the user's guide that comes with the SNMP Subagent. - Make sure the network card on the laptop is configured correctly.
Cannot log into Ethernet switch	- Make sure you are connected to the correct Ethernet port. (One Ethernet switch, it is the port marked Console) - Make sure you have the correct login ID and password. See the user's guide that comes with the Ethernet switch. - Make sure the network card on the laptop is configured correctly.
Cannot log into media server	- Make sure you are connected to the Services Ethernet port. (Default is port 2 [Eth1] on the back of the server). - Make sure you are using a crossconnect cable between the laptop and server. - Make sure the ARP cache is cleared on the laptop. In an MS-DOS window, type **arp -d 192.11.13.6** and press **Enter**. - Make sure you have connectivity. In an MS-DOS window, type **ping 192.11.13.6** and type **Enter**. - Make sure the NIC on the laptop is configured correctly.
Cannot access Avaya Installation Wizard	- Make sure you are plugged into the Services port (2 [Eth1]) - Make sure you are using the correct IP address: 192.11.13.6 - Make sure you are using the correct login and password. - Make sure the NIC on the laptop is configured correctly.
Cannot use SAT commands	- Make sure you are using the correct IP address: 192.11.13.6 and port (5023) - Make sure you are using the correct login and password.
Cannot ping out to customer's network	- Make sure that in the LAN security settings that "output from server" for icmp is enabled.
Cannot ping media server from customer's network	- Make sure that in the LAN security settings that "input to server" for icmp is enabled.
Cannot access media server remotely	- Make sure in the LAN security settings that "input to server" are checked for telnet (Linux commands), https (Web access), and def-sat (SAT commands access). The LAN security settings can be changed on the Web interface with a direct connection to the media server.
LED display on IPSI is flashing	- IPSI LED has not been programmed with switch and location (DHCP) - IPSI LED has not had an IP address assigned to it (static IP addressing)
Cannot access IPSI for static addressing	- Make sure you are plugged into the Services (top) port on the IPSI. - Make sure the ARP cache is cleared on the laptop. In an MS-DOS command window, type **arp -d 192.11.13.6** and press **Enter**.

Problem	Solution
No "V" on IPSI LED	- IPSI is not connected to Ethernet switch or network. Connect cable to bottom port on IPSI faceplate and to the Ethernet switch or the customer's network. - Make sure port on Ethernet switch assigned to that IPSI is enabled.
"V" on IPSI LED is not filled in	- IPSI does not have an IP address assigned to it. - IPSI has not been administered.
Get alarm when first connect to IPSI	- IPSI does not have current firmware. Upgrade firmware.

Installing the license and Avaya authentication files

Problem	Solution
Cannot get files from RFA site	- Provide the correct SAP number. - Provide the serial number for the reference IPSI
License file will not install	- Make sure there are not two license files on the server. If so, delete one of them. - May have corrupt file. Download file again from RFA site. - Upload using binary mode.
Media server is in no license mode	- Normal situation when license file is first installed because it cannot see the IPSIs; they do not have IP addresses yet. - After 30 minutes, license has not located reference IPSI. In a SAT session, type **reset system 1** and press **Enter** to reset the 30-minute clock.
Cannot use administration commands	- May be in No License Mode because 30-minute timer has lapsed. In a SAT session, type **reset system 1** and press **Enter** to reset the 30-minute clock.
ASG does not work	- Re-install Avaya authentication files.

C Avaya RSA defaults

Table 2, RSA Default Table, on page 107 outlines the Avaya defaults that were administered in the factory. See the *Avaya Remote Supervisor Adapter Users' Guide* (555-245-702) for more detailed information pertaining to each RSA field.

CAUTION:

Executing the **Restore Defaults** option in the navigation pane removes the Avaya defaults. Avaya defaults can be restored manually using the information found in this document or by restoring the Avaya default file. The Avaya default file can be found at http://support.avaya.com or on the Communication Manager 2.0 CD for Linux Servers and Gateways. To restore the default file, use the steps outlined in the Configuration File section of the *Avaya Remote Supervisor Adapter Users' Guide* (555-245-702).

Table 2: RSA Default Table ***1 of 5***

Main Heading In The RSA Navagation Pane	RSA Field	Avaya Default
ASM Control/System Settings	**ASM Information**	
	Name	1000000000 (9 zeros)
	ID Number	1000000000
	Contact	No default configured
	Location	No default configured
	Server Timeouts	
	POST Watchdog	5 minutes
	O/S Watchdog	2.5 minutes
	Loader Watchdog	5 minutes
	Power off delay	0.5 minutes
	NMI reset delay	Disabled
	ASM Date and Time	
	Automatic DST update	Disabled
	GMT offset	+0.00
Tasks/Power Restart	Power-on Server At A Specific Time	
	Power on time	Not set
ASM Control/Login Profiles	Login Profiles	
	Login ID 1	Login: craft
	Authority Level	Read/Write

Table 2: RSA Default Table ***2 of 5***

Main Heading In The RSA Navagation Pane	RSA Field	Avaya Default
	Dialback status	Disabled
	Dialback number	Blank
	Login ID's 2 through 12	~not used~
	Global Login Settings	
	Modem connection logins	Enabled
	Lockout period after five login failures	Two minutes
	Remote Alert Recipients	
	Recipient 1 through 12	~not used~
	Alert Forwarding	
	Status	Not a gateway
	Global Remote Alert Settings	
	Remote alert retry limit	8 times
	Delay between retries	4 minutes
	Include event log with e-mail alerts	Disabled
ASM Control/Monitored Alerts		
	Critical Alerts	
	Hard disk drive	Enabled
	Multiple fan failure	Enabled
	Power failure	Enabled
	Tamper	Disabled
	Temperature	Enabled
	Voltage	Enabled
	VRM failure	Enabled
	Warning Alerts	
	Single fan failure	Enabled
	Temperature	Enabled
	Voltage	Enabled
	Redundant power supply	Disabled
	System Alerts	
	Boot failure	Enabled
	Loader timeout	Enabled
	O/S timeout	Enabled

Table 2: RSA Default Table ***3 of 5***

Main Heading In The RSA Navagation Pane	RSA Field	Avaya Default
	PFA	Enabled
	POST timeout	Enabled
	Power off	Enabled
	Power on	Enabled
	Monitored Local Events	
	Event log 75% full	Enabled
	Event log full	Enabled
	Remote login	Enabled
	Voltage	Enabled
	Redundant power supply	Enabled
	Temperature	Enabled
	Power off	Enabled
	Tamper	Disabled
	Fan failure	Enabled
	Power supply failure	Enabled
	DASD failure	Enabled
	PFA	Enabled
ASM Control/Serial Port		
	Baud rate	57600
	Parity	None
	Stop bits	1
	Dedicated to ASM	Enabled
	Initialization string	ATZ^M
	Dial string	ATDT
	Hangup string	ATHO^M
	Dial postfix string	^M
	Modem query	AT^M
	Factory settings string	AT&FO^M
	Auto answer	ATSO=3^M
	Caller ID string	Blank
	Escape guard	2.5 seconds
ASM Control/Network Interfaces	Ethernet	

Table 2: RSA Default Table ***4 of 5***

Main Heading In The RSA Navagation Pane	RSA Field	Avaya Default
	Interface	Enabeld
	DHCP	Disabled
	Hostname	Name of the server-RSA: Up to 63 characters in length
	Static IP Configuration	
	IP address	192.11.13.6
	Subnet mast	255.255.254.0
	Gateway address	0.0.0.0
	Data rate	Auto
	Duplex	Auto
	MTU	1500 bytes
	Burned-in MAC address	Burned-in at the factory and cannot be changed
	Local administered address	00:00:00:00:00:00
	PPP Over Serial Port	
	Interface	Disabled
	Local IP address	10.4.0.1
	Remote IP address	10.4.0.2
	Subnet mask	255.255.254.0
	Authentication	Chap then PAP
ASM Control/Network Protocols	SNMP	
	SNMP agent	Disabled
	SNMP traps	Enabled
	Community 1 through 3:	
	Name	No default
	Host Name/IP address 1	No default
	Host Name/IP address 2	No default
	Host Name/IP address 3	No default
	DNS	
	Interface	Disabled
	DNS server IP addr 1	0.0.0.0
	DNS server IP addr 2	0.0.0.0

Table 2: RSA Default Table ***5 of 5***

Main Heading In The RSA Navagation Pane	RSA Field	Avaya Default
	DNS server IP addr 3	0.0.0.0
	Host table 1 though 4	0.0.0.0
	SMTP	
	Server host name/IP address	No default
ASM Control/Remote Control Keys		
	Prefix Key Combination	Ctrl-]

Index

A

access media server
directly, 95
remotely over modem, 97
remotely over network, 97
accessing Maintenance Web Interface, 98
accessing the media server, 41
add
IPSI information, 72
media gateways, 70
administer
IPSI, 71
IPSI circuit pack, 61
TN2312BP IP Server Interface, 71
Advanced System Management
configuring, 54
alarm activation level
setting, 72
alarming
setting selected traps, 36
alarms, 87
enabling to INADS via modem, 80
enabling to INADS via SNMP, 80
setting, 55
viewing, 78
ARP cache
clearing, 39
attendant console
LEDs, 87
Avaya P333T Ethernet switch
configuring, 37
LEDs, 89
security alert, 37

B

back up
RSA configuration, 57
back up files, 78
to compact flash media, 78

C

change
RSA password, 53
circuit packs
LEDs, 87
clearing ARP cache, 39
command line interface, 98
compact flash drive
on S8500 Media Server, 78
compact flash media
backing up files to, 78
configuration
backing up, RSA, 57
configure
Advanced System Management, 54
Avaya P333T Ethernet switch, 37
maintenance adapter, 52
media server, 39, 69
modem, 46
network interface card (NIC), 49
RSA, 52
UPS, 34
connect
IPSI to media server, 61
to customer network, 28
connecting
hardware, 61
connection to LAN
verifying, 45
conventions, 10
customer network
connecting to, 28

D

date and time
verifying, 77
daylight savings rules
location, 77
setting, 76
DHCP IP addressing
IPSI circuit pack, 61
direct access to media server, 95
disconnecting from media server, 48
documentation, 27
downloading files, 21
downloading this book, 12
downloading updates from the Web, 12

F

faceplates
TN2312BP circuit pack, 90

H

hardware
connecting, 61
high-level overview of installation process, 31

I

inputing translations, 70
installation
    troubleshooting, 103
installation process
    high-level overview, 31
Installation Wizard
    using, 43
installing
    media gateways, 83
    software, 42
    translation file, 73
IPSI
    administering, 71
    LEDs, 90
    program switch ID and cabinet, 61
    verify circuit pack version, 67
IPSI information
    adding, 72
IPSIs
    enabling control, 67
    verify translations, 66

L

LEDs
    alarms, 87
    Avaya P333T Ethernet switch, 89
    checking network interface card (NIC), 48
    IPSI, 90
    S8500 Media Server, 88
    UPS, 90
license file
    testing, 86
license status,verifying, 67
light emitting diodes. See LEDs.
loader watchdog on RSA
    disabling, 40
    enabling, 60
location
    daylight savings rules, 77
    setting, 77

M

maintenance adapter
    configure, 52
    setting alarms, 55
Maintenance Web Interface, accessing, 98
media gateways
    adding, 70
    installing, 83
media server
    accessing, 41
    backing up to compact flash media, 78
    configuring, 39, 69
    disconnecting from, 48
    LEDs, 88
    powering up, 41
    registering, 81
    reset, 70
    telneting, 80
    verify connectivity, 66
media server connection to LAN
    verifying, 45
modem
    access to media server, 97
    configuring, 46
    connect to media server
        collocated, 29
        separated servers, 29

N

network interface card (NIC)
    checking LEDs, 48
    configuring, 49
    testing connectivity to network, 50

P

powering up media server, 41
pre-installation setup, 19

R

registering media server, 81
remote access to media server
    over modem, 97
    over network, 97
Remote Supervisor Adapter. See RSA.
reset media server, 70
RSA
    Advanced System Management, 54
    alarms, 55
    backing up configuration, 57
    change login ID, 53
    components, 26
    configure, 52
    defaults, 107
    disabling loader watchdog, 40
    enabling loader watchdog, 60
    login ID change, 53
    password change, 53
    setting auto answer, 59
RSA login ID
    change, 53
RSA password
    change, 53

S

S8500 Media Server
  LEDs, 88
safety labels, 13
saving translations, 70
security alert labels, 13
set
  alarm activation level, 72
  alarms, 55
  auto answer on RSA, 59
  daylight savings rules, 76
  location, 77
  selected traps (alarming), 36
  Telnet, 41
software
  installing, 42
static IP addressing
  IPSI circuit pack, 61

T

technical assistance, 16
Telnet
  setting up, 41
Telnet to media server, 80
terminal emulation, 98
  starting, 69
testing
  complete configuration, 85
  connectivity to network, 50
  license file, 86
  TN2312BP, 85
TN2312BP
  administering, 71
  faceplate, 90
  LEDs, 90
  program switch ID and cabinet, 61
  testing, 85
translation file
  installing, 73
translations
  backing up, 78
  inputing, 70
  saving, 70, 78
  verifying, 75
troubleshooting
  media server installation, 103
typography, 10
typography conventions
  commands, 11
  field names, 12
  keys, 11
  system output, 12
  user input, 11

U

UPS
  configuring, 34
  LEDs, 90
  security alert, 34
  single control network, 35
  SNMP module, 34
using this documentation, 9

V

verify
  connectivity to media servers, 66
  date and time, 77
  IPSI circuit pack version, 67
  IPSIs translated, 66
  license status, 67
  media server connection to LAN, 45
  translations, 75
view
  alarms, 78